[The Complete] Management Solution
For Your Network

PRODUCT MANUAL

ManageWise® 2.6

InocuLAN 4 for Windows NT Guide

ManageWise®
MANAGEMENT SOFTWARE

Novell®

disclaimer

trademarks

Credits

Written by Christopher B. Welch

Edited by Alex Chen, Victor Tsui, Thomas Mueller, Carl Oddo, Mark Lewis, Paul Nash, and Stone JyhKwei Shih

Product Support

If you have any questions about this product, please contact us at one of the following:

USA, Canada, Asia, Latin America: 3 Expressway Plaza Roslyn Heights, New York 11577 USA	Main Voice Number: Technical Support: Tech Support FAX: BBS: CompuServe: World-wide Web: FTP Server: InfoFax System:	516-465-4000 800-CHEY-TEC Mon-Fri 8:00 am- 8:00 pm EST Mon-Fri 8:00 pm-10 pm EST (Callback only) Sat/Sun 10:00 am-4:00 pm EST (Callback only) 516-465-5115 516-465-3900 GO CHEYENNE http://www.cheyenne.com/ ftp.cheyenne.com 516-465-5979 (Outside of North America you must use a fax machine's telephone.)
European Headquarters: Cheyenne Software S.A.R.L. Bel Air Building 58 rue Pottier 78150 Le Chesnay, France	Southern Europe Tech Support: Tech Support (FAX Hot Line): BBS: Infofax:	+33-1-49-93-90-34 Mon-Fri 09:00 - 17:00 +33-1-39-23-18-69 +33-1-39-23-18-60 +33-1-39-23-47-00
Germany: Cheyenne Software Deutschland Bayerwaldstr. 3 81737 Munich, Germany	Central and Eastern Europe Tech Support: Tech Support FAX: BBS (28800,N,8,1): BBS ISDN 64kB (v110, v120):	+49-69-920321-80 Mon-Fri 09:00 - 17:00 +49-89-627241-41 +49-89-627241-80 +49-89-627241-85
England: Cheyenne Software (UK) LTD Furness House 53 Brighton Road Redhill, Surrey, England RH1 6PZ	Northern Europe Tech Support: Tech Support FAX: BBS:	+44 (0) 990 239606 Mon-Fri 09:00 - 17:00 +44 (0) 990 785783 +44 (0) 990 143012
Japan: Cheyenne Software K.K. Sumitomo Fudosan Sanbancho Bldg. 3F, 6-26, Sanban-cho, Chiyoda-ku Tokyo 102, Japan	Voice: FAX:	+81-3-3222-3760 +81-3-3222-3762
Taiwan: Cheyenne Software, Taiwan Branch Room C, 4th Floor 170 Tun Hua North Road Taipei, Taiwan	Voice: FAX:	+886-2-545-5611 Mon-Fri 9 am- 5 pm +886-2-545-5616

Training

For the convenience of our customers, Cheyenne University has established a network of Authorized Cheyenne Education Centers and Authorized Cheyenne Instructors. For the latest course descriptions and schedules:

· Customers in U.S. / Canada, call: 800-243-9272
· Customers in Europe, Africa, and Middle East, call: +33-1-39-23-18-80
· Customers in Australia, call +61-2-9591944
· Customers in Japan, call: +813-3222-3750
· Customers in Taiwan and Asia, call: +886-2-7951092
· Customers in other areas, call: +1-516-465-4000

CONTENTS

Getting Started

Protecting Your Windows NT Network

Configuring Services, Logs and Broadcasts

Automatic Download, Distribution and Update

Alerting Users When a Virus is Detected

GETTING STARTED

This chapter explains how to get started using Cheyenne InocuLAN 4 for Windows NT.

In this chapter, you will learn:

About InocuLAN 4 for Windows NT

Cheyenne InocuLAN 4 for Windows NT is a powerful, second-generation anti-virus solution for your Windows NT network. It is part of the Cheyenne AntiVirus family of products, including desktop versions that protect your workstations running under Windows 95, Windows 3.x, DOS, and Macintosh. Available options provide protection for Lotus Notes and Microsoft Exchange messaging systems. InocuLAN is also available for Novell NetWare.

InocuLAN features

InocuLAN 4 for Windows NT protects your Windows NT enterprise with an unmatched set of powerful features.

- **Real-time protection** provides a hands-free, continuous barrier against viruses that stops infections before they can spread. InocuLAN uses a number of real-time components to protect all avenues of entry into the Windows NT enterprise, including:
- **Real-time Scanning Mode:** All files going to and from the server are scanned for viruses, including compressed files. With InocuLAN real-time in operation, viruses won't spread through your network.
- **Virus Wall:** A little-known but very dangerous security leak that many anti-virus products can't stop is the infection of a server by a workstation. InocuLAN stops any infected file from being copied to a server and replacing the clean version of the file, thereby keeping enterprise security intact.
- **Virus Quarantine:** Users who try to copy infected files to a server are automatically suspended from the machine, isolating the infection before it can spread. A message is sent listing the name of the user who tried to move an infected file.
- **Floppy-drive protection:** Floppy diskettes are the most common source of virus infections, and InocuLAN fully protects your enterprise from floppy-based viruses. As soon as a floppy diskette is accessed,

such as looking at the disk contents in My Computer, InocuLAN scans the boot sector, preventing the spread of dangerous boot viruses. When a file is opened or copied from the floppy, InocuLAN scans it before it moves to the hard drive.

- **CD-ROM protection:** Because you will want to protect your environment from viruses when you download data or access data on CD's, you can now prevent viruses from being copied onto your machine.
- **Network drive protection:** Another little-understood but common way of spreading viruses happens when files are copied from one mapped drive to another. Even though no file passes through the hard drive of the local machine, InocuLAN will still scan all files moving between mapped drives.
- **Internet-enabled:** The newest source of virus infections is the Internet. As users gain nearly limitless access to computers world-wide, the chances of downloading infected files grows exponentially. With InocuLAN running, all file downloads are automatically scanned for viruses *before* they can infect a machine. This includes support for compressed files. InocuLAN works with browsers from NetScape and Microsoft.
- **Groupware Messaging AntiVirus options:** More than ever, companies are communicating electronically. As more data is being exchanged, more viruses are spreading by hiding in mail attachments and database files. InocuLAN is the only product that can protect your Lotus Notes

or Microsoft Exchange mail systems with its messaging options. Even attached ZIP files are scanned. (Cheyenne is also developing messaging protection for GroupWise, which will be available soon.)

- **Support for Windows NT 4.0**. Includes shell extension integration, providing right-click scanning from any volume, folder, or file.
- **Multi-platform support:** InocuLAN NT versions for Intel, Digital Alpha, NEC MIPS, and Motorola Power PC.
- **Microsoft BackOffice support:** InocuLAN NT carries the "Designed for BackOffice" logo.
- **NCSA Certification** ensures protection against 100% of the computer viruses in the wild, as certified by the National Computer Security Association (NCSA).
- **New Multiple Source Browser**: A new Explorer-like browser makes viewing and selecting servers, directories, and files faster and easier. Multiple sources can be selected for scanning.
- **NetWare domain management** lets you administer your InocuLAN NetWare servers through the Windows NT console.
- **Real-time Copy Cure option**: Makes a copy of the infected file before curing it.
- **Automatic Software Download, Distribution and Update:** Hands-free downloading and distribution of the latest signature files and search engines using modem or FTP downloads. Supports multi-language, multi-platform networks.

- **Point-to-Point Management**: InocuLAN Servers can be managed by entering the machine name. This mean InocuLAN can communicate with all InocuLAN servers, even across segmented LANS where broadcasts are filtered out.
- **Compressed Files**: Scans compressed files and internet downloads in .ZIP, .ARJ, and Microsoft compressed formats.
- **Scheduled Scanning** allows administrators to scan networked servers at predetermined times.
- **Domain Support** allows you to configure servers into InocuLAN domains. Multiple servers can be configured at one time.
- **Updated Alert System** immediately notifies selected users of a virus threat through network broadcast, print queue/ trouble ticket, Microsoft Mail, Microsoft Exchange, SNMP, and pager.
- **Remote System Event Log Support**: Uses Alert 4.0 to forward Alarm information to remote server's system even logs.
- **Flexible Reporting** includes scanning results, virus incidents, configuration changes, and status reports. Reports are completely automated and centralized across InocuLAN domains.

How does InocuLAN work?

Cheyenne InocuLAN scans files on your workstation, using signature checking and a rules-based polymorphic analyzer virus scanner to detect known viruses. If a virus is detected, you decide how the infected file should be handled. You can delete, rename, cure, move, purge or report an infected file.

Virus prevention methods

Currently, InocuLAN uses four techniques to detect computer viruses:

- **Integrity Checking**- determines if the program's contents have changed due to a virus attaching itself to a program. InocuLAN integrity checking primarily to check the integrity of the Critical Disk Area information.
- **Rules-based, Polymorphic Analyzer Detection**- observes the way programs behave to detect suspicious program behavior.
- **Interrupt Monitoring**- observes all program system calls in an attempt to stop the sequence of calls which may indicate virus actions.
- **Signature Scanning**- method uses a unique set of hexadecimal code, the virus signature, which a virus leaves within an infected file. By searching the program files armed with these codes, the signature scanner can detect that known virus. Signature file updates are free of charge and available over CompuServe, the World Wide Web, Cheyenne's BBS and FTP sites worldwide.

Installing InocuLAN 4.0 for Windows NT

System requirements

To install and use InocuLAN 4 and Alert on your Windows NT computer, the following hardware and software requirements must be satisfied:

Machine Type	80486 DX or higher PC, Alpha, MIPS or Power PC.
Operating System	Windows NT version 3.51 or higher
Minimum System Memory	16 Megabytes minimum, 32 megabytes recommended
Disk Space	8 Megabytes

Installation

NOTE: Please read the Release Notes fully before installing.

To install InocuLAN 4.0 for Windows NT:

1. **Insert the InocuLAN Installation CD-ROM into the machine's drive.**

2. **Choose *Run* from the File Menu in the Windows NT Program Manager.**

   The Run dialog box opens.

3. **In the Run dialog box, type D:SETUPCD (This is assuming that your drive D is the CD-ROM drive) and then click OK. The Master Installation Option screen will appear. Make your selection and continue.**

4. **The InocuLAN Welcome screen will appear, listing the system requirements. Click Next to continue.**

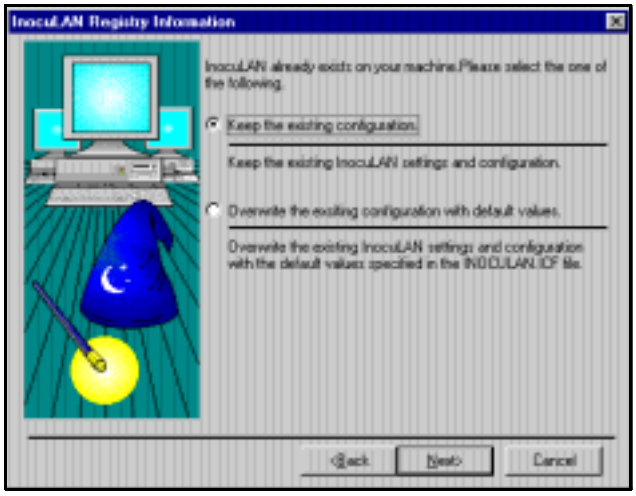
5. **The License screen appears:**

If you are using a CD Key for licensing, enter the key in the appropriate spaces. If you are using a license file, direct InocuLAN to the file's location using the Browse button.

Click Next to continue.

6. **The User Information screen appears. Enter your name and company on the screen and click Next to continue.**

7. If you have a previous version of InocuLAN on the machine, the Registry Information screen will appear.



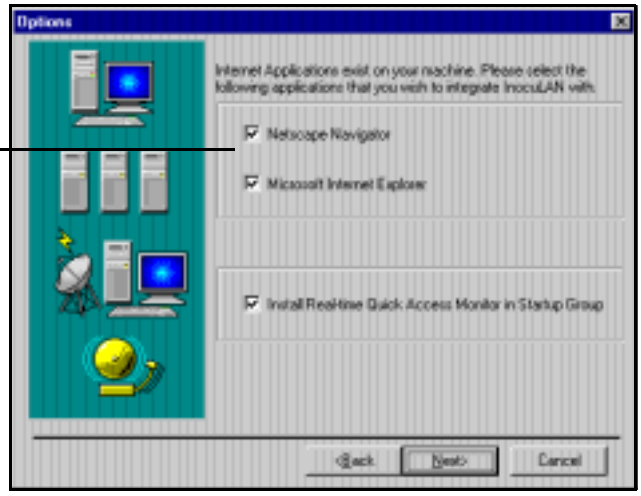
If you wish to keep your previous InocuLAN information, such as scan logs and domain configurations, choose *Keep the existing configuration*.

To overwrite previous information, select *Overwrite the existing configuration with default values*. This will set all values to the InocuLAN default settings.

Click Next to continue.

7. The InocuLAN Options screen appears:

These fields will be grayed out if you do not have an applicable browser on your machine.

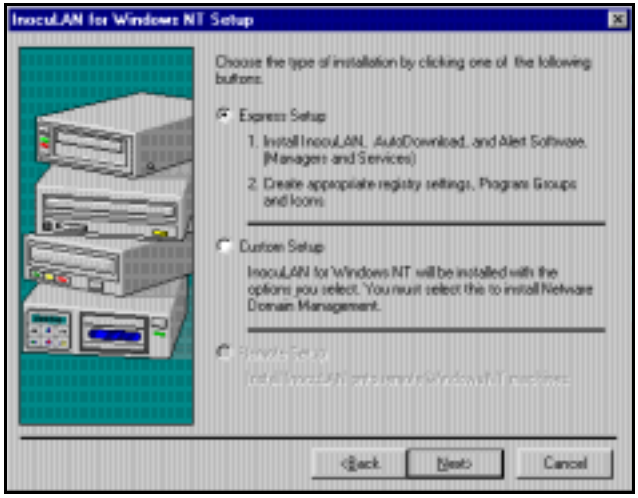


InocuLAN provides automatic scanning of internet downloads. To install the internet helper applications, select the applicable browser(s).

The Real-time Monitor can be accessed from the Windows NT 4.0 system tray via the Quick Access Monitor. If you would like the Quick Access Monitor to appear on startup, select the installation option.

Click Next to continue.

10. Choose either Express Setup or Custom setup.



Express setup will install all major InocuLAN components. Custom Setup will allow you to choose from the following:

- *Install all Alert files.*
- *Install AutoDownload (Server and Manager).*
- *Install InocuLAN for Windows NT Manager*
- *Install InocuLAN for Windows NT Server.*
- *Install NetWare Domain Management Capability*

NOTE: The only way to install the NetWare Domain Management capability is through Custom Setup.

Click Next to continue.

9. The Select Directory screen appears. Click Next to accept the default values, or enter a new directory and path for the installation.

10. **A message screen will note that all necessary information has been collected. At this point, you may still click the Back button to change your installation settings.**

    Click Finish to begin the product installation.

    InocuLAN will begin copying files to your hard drive. You will be prompted when the installation is complete. Restart your InocuLAN machine for all settings to take effect.

Remote Setup for InocuLAN

You can run remote setup to install InocuLAN to a remote Windows NT 3.51 or 4.0 machine from a source Windows NT machine.

The entire InocuLAN configuration on the target NT machine is derived from the INOCULAN.ICF file, which you must configure before remotely installing InocuLAN.

NOTE: You should edit the InocuLAN.ICF file using a text editor. A word processor will corrupt the file.

Running a Remote Setup for Windows NT

Use the following procedure to install InocuLAN 4 on remote NT servers or workstations.

1. **Using a text editor, edit the settings of the parameters in your source server's INOCULAN.ICF file listed in the following tables:**

InocuLAN.ICF file settings for Remote Setup

Parameter	Default	Purpose
[Components] DomainManagement=<0 or 1>	1	Installs domain manager files (SERVICE.DLL and DOMAIN.DLL).
[IconCreation] CreateAllIcons=<0 or 1>	1	A value of "0" specifies that the icons and program group for InocuLAN are not created in the Program Manager or in the start menu's program groups, while a value of "1" creates the icons and group. If a user does not have administrator rights to the client machines, he should set the value to "0" as he will not be allowed to create the program groups.
[Settings] DomainName=	NONE	If you want to install this machine to an InocuLAN domain, you must set the value to the name of the domain. **Note:** You must enter this value in upper-case letters.

InocuLAN.ICF file settings for Remote Setup		
Parameter	**Default**	**Purpose**
[Settings] MasterServer=	NONE	If you want to install this machine to an InocuLAN domain, you set the value equal to the name of the machine that is the InocuLAN Master Server for the InocuLAN domain in this line. **Note:** You must enter this value in upper-case letters.
[Settings] BCastType=<0, 1, 2, or 3>	3	Enter a value to specify the broadcast method. "0" - Disables broadcasts. "1" - Mailslot - Use this method if you are not using an IP network. "2" - TCPIP - This setting is recommended if you are in an IP only environment. "3" - Both - This method will broadcast to IP addresses and mailslots in your network. **Note:** For greater efficiency, we recommend that you select "1" or "2" depending on your network.
[Settings] BCastInterval=	180 **Note:** The local broadcast interval is 1/3 of this value.	This value specifies the "Active Server Timeout". A remote InocuLAN machine will appear grayed out in the Domain Manager if the Local InocuLAN machine does not receive a broadcast within this interval. You should use the following equation to set this value: (number of machines / 50) * 180 **Note:** This value needs to be constant for all machines across your network.
[Settings] AutoDiscoveryType=<0 or 1>	1	"0" - (pre-build 48 method) Discovers subnets by reverse Mask calculations based upon IP addresses. This method can generate false values in environments that have multiple masks. "1" - (build 48 and above) Discovers subnets by using an RPC ping. **NOTE:** If you have more than one subnet mask on your network, we recommend that you do not change this value. If you have only one subnet mask you can change the value to "0" which will take less time to discover the other InocuLAN machines in your network.

InocuLAN.ICF file settings for Remote Setup		
Parameter	**Default**	**Purpose**
[Settings] AutoDiscoverInterval=	24 (hours)	Value in hours for the interval in which InocuLAN autodiscovers other InocuLAN machines in your network. If you set this value equal to "0", InocuLAN does not perform Autodiscovery. **Note:** Set this value to "0" if you are rolling out pre-configured table files or using the following equation to calculate the value: (number of machines / 100) * 24.
[PreinstalledTables] BraoadcastTables=<0 or 1>	0	"0" - The preconfigured tables, DOMAIN.TBL, IPNET.TBL, and IPMASK.TBL, are not copied from the setup directory to the InocuLAN target directory. "1" - The preconfigured tables, DOMAIN.TBL, IPNET.TBL, and IPMASK.TBL, are copied from the setup directory to the InocuLAN target directory. **Note:** This option is used if you want to roll out a set of pre-configured tables. If you set this value to "1", you should set the "AutoDiscoverInterval" to "0" to prevent InocuLAN from altering these tables during the process of Autodiscovery.

Real-time Scanner Settings

[Real Time]		
Parameter	**Default**	**Purpose**
ExeOnly=<0, 1, or 2>	1	Enter "0" to scan all files, "1" to scan files with the default extensions, or "2" to scan all files save those with the default extensions.

[Real Time]		
Parameter	**Default**	**Purpose**
Method=<1 through 7>	0	You select from one of the following actions upon detection of viruses: 0 - Report only 1 - Delete the infected file 2 - Rename the file with the .AV* extension (subsequent files with the same initial characters will be named .AV0, .AV1, .AV2, etc. 3 - Copies infected files to a temporary directory, then cures the file in the original location. 4 - Moves files to a temporary directory. 5 - Purges the files from your local drives destroying them utterly. 6 - Moves infected files from the original directories to a temporary directory and renames the files with the .AV* extension (subsequent files with the same initial characters will be named .AV0, .AV1, .AV2, etc.
Mode=<0, 1, or 2>	1	You specify one of three scanning methods to use for Real-time scanning: 0 - fast scan (scans only the headers and footers of files) 1 - secure scan (scans the entire file for any known viruses) 2 - reviewer scan (scans the entire file for any virus-like patterns)
Direction=<0, 1, 2, or 3>	3	Enter a value to specify whether to scan incoming or outgoing files on your hard drive: 0 - The Real-time monitor is disabled 1 - Outgoing files are scanned. 2 - Incoming files are scanned. 3 - Both incoming and outgoing files are scanned.
bFirewall=	0	Enter a value to enable or disable the “Virus Wall”. “0” - Protection is turned off. “1” - Protection is enabled.
bFloppyDrive=<0 or 1>	1	Enter a value to enable or disable Real-time scanning on floppy drives. “0” does not scan the floppy drive. “1” scans the floppy drive.
bNetworkDrive=<0 or 1>	0	Enter a value to enable or disable Real-time support on mapped drives. “0” does not scan the network drive. “1” scans the network drive.

[Real Time]		
Parameter	**Default**	**Purpose**
bEnforcement=<0 or 1>	0	Enter a value to specify whether or not to quarantine users when they copy viruses. "0" - Users who copy viruses are not quarantined. "1" - Users who copy viruses are quarantined.
bGetUserName=<0 or 1>	1	Enter a value to specify whether or not file access for users is tracked. "1" - File access for users is tracked. "0" - File access for users is not tracked.
RealtimeRefreshHrs=	1 (hour)	Enter a value in hours for the interval after which InocuLAN saves statistical information to the Registry.

Local Scanner Settings

[Local Scanner]		
Parameter	**Default**	**Purpose**
BeepOnDetect=<0 or 1>	1	Enter a value to specify whether or not your computer provides an audible warning when a virus is detected. “0” does not generate an audible warning. “1” generates an audible warning.
ScanExeOnly=<0, 1, or 2>	0	Enter a value to specify whether to scan all files, executable files with default extensions, or all files save executable files with default extensions. “0” will scan all files. “1” scans executable files with default extensions. “2” scans all files save executable files with default extensions.
ScanArchives=<0 or 1>	1	Enter a value to specify whether or not the Local Scanner scans compressed files. “0” does not scan compressed files. “1” scans compressed files.
ScanBoot=<0 or 1>	1	Enter a value to specify whether or not to scan the boot sector area of your hard disk. “0” - the boot sector is not scanned “1” - the boot sector is scanned.
ScanFiles=<0 or1>	1	Enter a value to specify whether or not to scan only the boot sector area of your hard disk. “0” - files are scanned. “1” - only the boot sector is scanned.

[Local Scanner]		
Parameter	**Default**	**Purpose**
InfctAct=<0 through 6>	0	Enter a value to specify what actions are taken on infected files by the local scanner. 0 - Report only 1 - Delete the infected file 2 - Rename the file with the .AV* extension (subsequent files with the same initial characters will be named .AV0, .AV1, .AV2, etc. 3 - Copies infected files to a temporary directory, then cures the file in the original location. 4 - Moves files to a temporary directory. 5 - Purges the files from your local drives destroying them utterly. 6 - Moves infected files from the original directories to a temporary directory and renames the files with the .AV* extension (subsequent files with the same initial characters will be named .AV0, .AV1, .AV2, etc.
ScanMode=<0, 1, or 2>	1	Enter a value to specify what type of scan the Local Scanner uses: 0 - fast scan (scans only the headers and footers of files) 1 - secure scan (scans the entire file for any known viruses) 2 - reviewer scan (scans the entire file for any virus-like patterns).
AutoDisplay=<0 or 1>	1	Enter a value to specify whether or not the results dialog is displayed after the scan job is performed. “0” - does not display the results dialog box. “1” - displays the results dialog box.
ExtName=	“APP*BIN*COM*DLL*DOT *DOC*DRV*EXE*OVL*OVR*PRG *SYS*VXD*XLT*XLA*XLS*XLW*”	Lists of the types executable file types by extension that are scanned by the Local Scanner.
SkipExtName=	“BTR*DBF*SBF*DB*MDB*MDX* NDX*”	Lists of the types executable file types by extension that are not scanned by the Local Scanner.
ArcExtName=	ZIP*ARJ*LHA*LZH*MIM*UUE*	Enter a value to specify the different types of compressed files (by type) the Local Scanner scans.
LotusNotesExtName=	“NSF*NTF*”	Enter the default extensions for the Lotus Notes database files and templates you want to scan. **Note:** This setting only applies when the AntiVirus Agent for Lotus Notes is installed.

[Local Scanner]		
Parameter	**Default**	**Purpose**
IncrementalScan=<0 or 1>	0	Enter a value to specify whether or not you want to scan only the messages created since the last scan (**1**) or all messages (**0**). **Note:** This setting only applies when the AntiVirus Agent for Lotus Notes is installed.
NotifyOwner=<0 or 1>	1	Enter a value to specify whether or not you want notifications sent to mailbox owners who possess infected e-mail. "0" - Users who possess infected e-mail are not notified. "1" - Users who possess infected e-mail are notified. **Note:** This setting only applies when the AntiVirus Agent for Lotus Notes is installed.
NotifySender=<0 or 1>	0	Enter a value to specify whether or not you want the users who send infected e-mail to other users notified. "0" - Users who send infected e-mail do not receive messages. "1" - Users who send infected e-mail receive messages. **Note:** This setting only applies when the AntiVirus Agent for Lotus Notes is installed.
bNotifyAdministrator=<0 or 1>	0	Enter a value to specify whether or not the e-mail Administrator is notified when a virus is detected in an e-mail. "0" - The administrator does not receive a message when a virus is detected. "1' - The network administrator receives a message upon detection of a virus. **Note:** This setting only applies when the AntiVirus Agent for Lotus Notes is installed.
bAttachInfoFile=<0 or 1>	1	Specify whether or not a virus report is attached to your notifications. "0" - A virus report is not attached to your messages. "1" - A virus report is not attached to your messages. **Note:** This setting only applies when the AntiVirus Agent for Lotus Notes is installed.

[Local Scanner]		
Parameter	**Default**	**Purpose**
ScanAfter=<0 or 1>	0	Enter a value to specify whether or not to allow virus scans only after a given date. "0" - Virus scans are allowed any time. "1" - Virus scans are only allowed after a give date. **Note:** This setting only applies when the AntiVirus Agent for Lotus Notes is installed.

2. **In the Windows NT 4.0 or 3.51 Program Manager, do one of the following:**

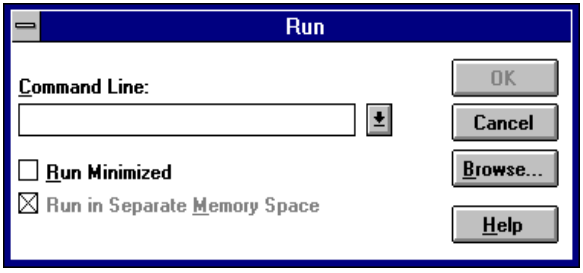
   „ **For Windows NT 4.0** - Click on the *Start* button, then select *Run*.

   the *Run* dialog box appears.

   Click on the *Browse* button, browse your CD-ROM drive, select the *SETUP.EXE* file, then click on the *OK* button.

   „ **For Windows NT 3.51** - Click on the *File* menu, then select *Run*.

   The *Run* dialog box appears.



   Click on the *Browse* button, browse your CD-ROM drive, select the *SETUP.EXE* file, then click on the *OK* button.

3. **Read the contents of the *Welcome* dialog box (especially the *Requirements* section), then click on the *Next* button.**

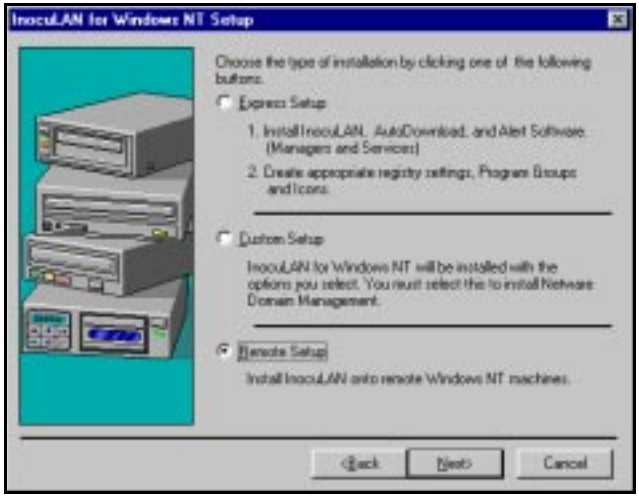
The *InocuLAN for Windows NT Setup* dialog box appears.

4. **Click on either the *Install from CD Key* option button to type in a valid CD Key or the *Install from License file* option button to browse and select your license file, then click on the *Next* button.**

   The *User Information* dialog box appears.

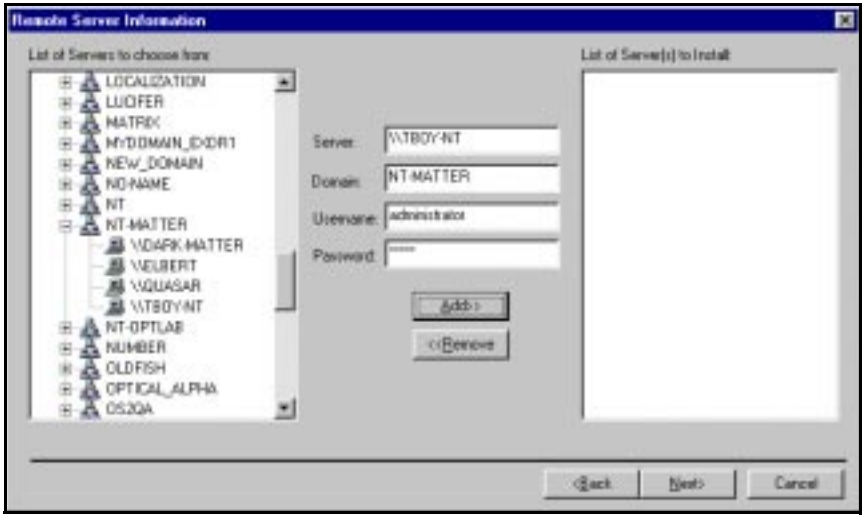
5. **Enter your name and the name of your company, then click on the *Next* button.**

   The *InocuLAN for Windows NT* dialog box appears.



6. **Click on the *Remote Setup* button, then click on the *Next* button.**

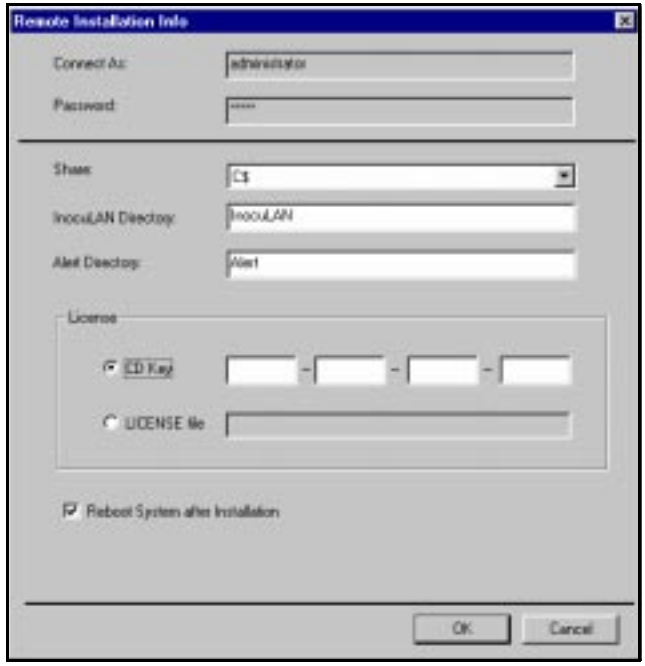
   The *Remote Server Information* dialog box appears.



7. **In the *Remote Server Information* dialog box, browse the remote server to which you want to install InocuLAN, provide the security information (server name, domain, user name for logging in, and valid password), then click on the *Add* button.**

NOTE: You must have Administrator's access on the remote machine.

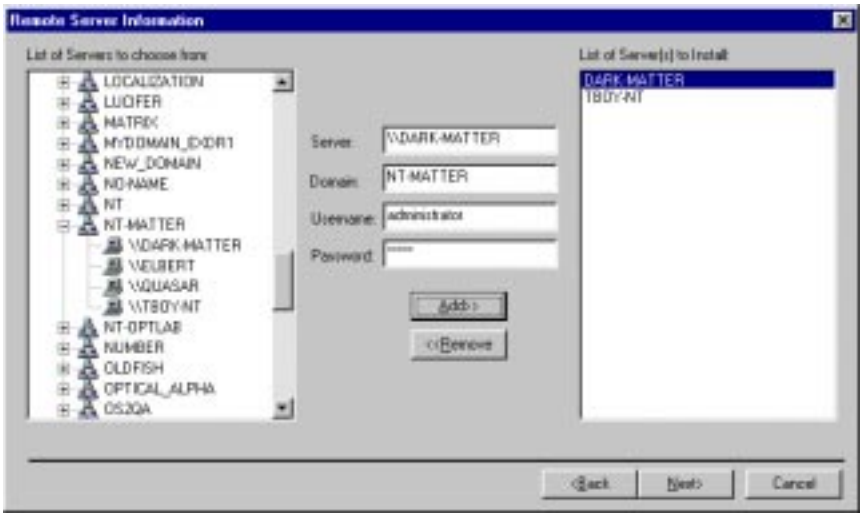
The *Remote Installation Info* dialog box appears.



8. **In the *Remote Installation Info* dialog box, view the security credentials in the *Connect As:* and *Password* list boxes, select the appropriate share on the remote NT machine in the *Share:* drop-down list, select an alternate for InocuLAN and Alert program files in the *InocuLAN Directory:* and *Alert Directory:* edit boxes respectively (if you do not want to accept the defaults), click on the *CD Key* option button to enter a 20-digit CD Key or click on the *License File* option**

button to type the path to your license file, click on the *Reboot System after installation* check box if you do not want to reboot the system after you install the program files, then click on the *OK* button.

The NT server or workstation is listed in the *List of Server(s) to Install:* list window indicating that InocuLAN will be installed on that NT machine.



NOTE: You can repeat this process for the NT machines on your network on which you want to remotely install InocuLAN.

9. **When you are done adding the NT machines on which you want to install InocuLAN into the *List of Server(s) to Install:* list window, click on the *Next* button.**

   The *InocuLAN for Windows NT Setup* dialog box appears, informing you that you have provided all of the information you need to remotely set up InocuLAN.

10. **Click on the *Finish* button.**

The InocuLAN program files are pushed out to your remote NT servers and workstations.

Chapter 2

PROTECTING YOUR WINDOWS NT NETWORK

This chapter explains how to scan and safeguard your Windows NT network.

In this chapter, you will learn:

Protecting your NT Network with the Domain Manager

The Domain Manager lets you group servers into logical units called InocuLAN Domains. Server management can be done at the domain level, so information entered once applies to all servers in the domain. Servers can also be managed individually within a domain.

There are several steps to take to best ensure network protection. Briefly, these steps are as follows:

- Group your NT machines into InocuLAN domains.
- Configure and start up InocuLAN's Real-time Monitor for each domain. This will immediately protect your network from new virus infections.
- Scan the entire network to locate any viruses that may have infected your machines before real-time monitoring was turned on.
- Schedule full domain scans to run at a regular interval. While InocuLAN's multiple real-time capabilities effectively stop new virus infections, there are two reasons you should also run a scheduled scan.

If for any reason real-time monitoring is turned off on a particular machine, that machine is vulnerable to infection until the monitor is turned back on. A periodic scan of the machine will locate any viruses that may have infected the machine while real-time was shut down.

New viruses are always being created. Cheyenne Software provides monthly virus signature file updates to locate the latest virus threats. It is possible that a new virus can infect your machine before the latest signature file is available. Running a domain scan as soon as a new signature file is available ensures that new viruses are detected as soon as possible.

- Set up InocuLAN's automatic file download and distribution system, to keep your InocuLAN network up-to-date.

Setting up domain-based network protection

The following pages will explain how to set up an InocuLAN domain, start and configure real-time virus protection, and scan your network servers. In our example, we will show how to create and manage an InocuLAN domain of five Windows NT servers.

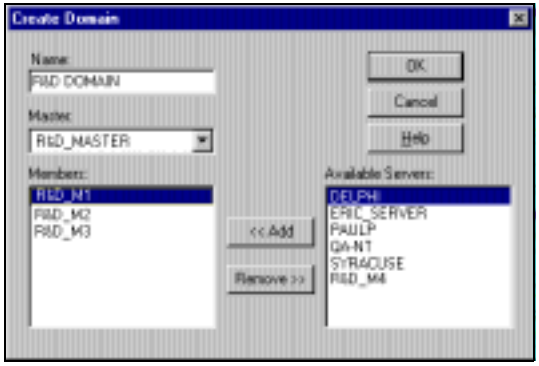
Creating the domain

The first step is to set up the InocuLAN domain.

1. **Open the Domain Manager.**

2. **Click the Create Domain button.**

   The Create Domain window will show you which servers are available to place into a domain. A machine must have InocuLAN installed to be seen in the Available Servers list.



3. **In this example, we will create an InocuLAN domain called R&D DOMAIN. Enter this name in the Name field.**

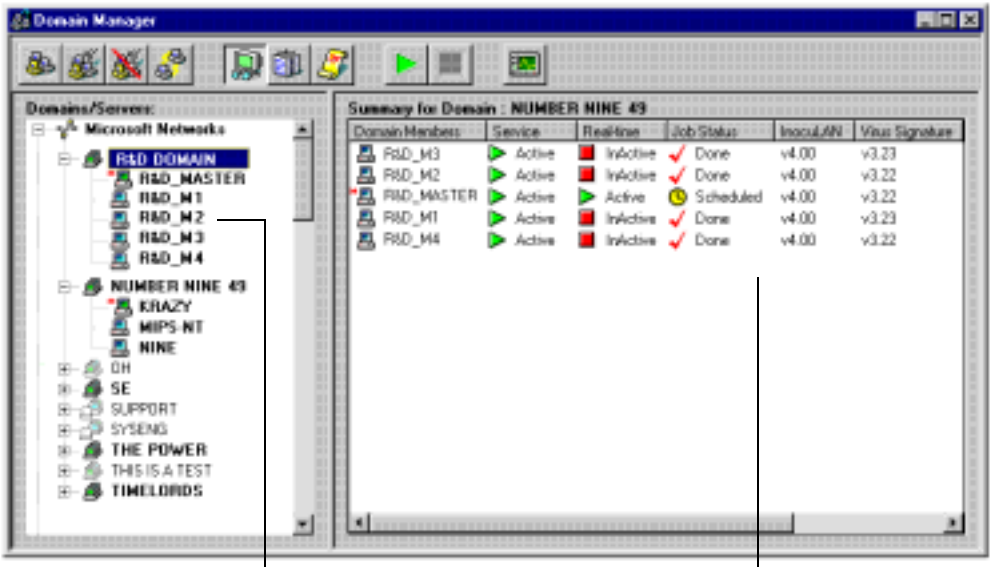
4. **Each InocuLAN domain requires a master server. The master server sends management information to all other member servers in the domain. Any available**

server can become the master server. Select your master server using the drop-down list in the Master field. For our example, we have selected R&D_MASTER.

Picking the master server: There are 3 factors to consider when choosing a master server.
In a mixed environment of InocuLAN versions 1.01 and 4, the master server *must* be an InocuLAN 4 machine. The master server will contain scanning logs for all machines in the domain. The log will grow over time, so you shouldn't pick a machine that is very short of disk space. The master server will collect Alerts from its members and send them out via the Alert manager. If you wish to use paging, you must select a server that has a modem.

5. **Add member servers to the domain by highlighting them in the Available Servers field and clicking Add. In our example, we are adding four other servers into the domain, creating a total InocuLAN domain consisting of five Windows NT machines.**

   Upon completion, R&D DOMAIN and all the member servers will be seen in the Domain Manager window.



The newly created InocuLAN domain is shown here.

Information about machines in the domain is shown in the Summary window. If you click on a machine within the domain, you will see additional details about that machine.

Setting up Real-time protection

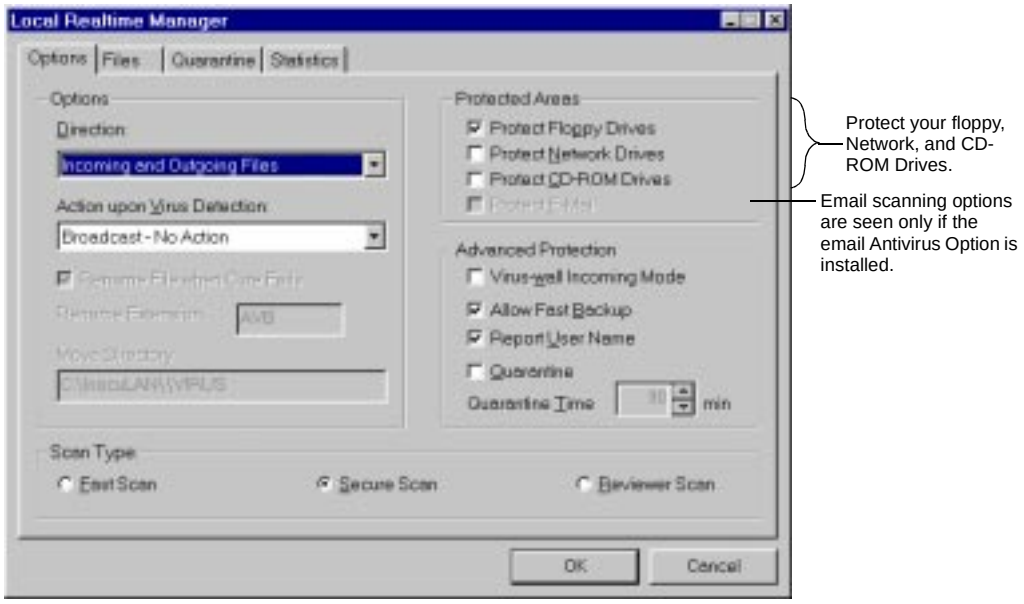
Now that five servers have been logically grouped into R&D DOMAIN, we want to immediately protect them from viruses by configuring real-time protection.

Configuring the Real-time Monitor

1. **Highlight R&D DOMAIN in the Domains/Servers window.**

2. **Click the Real-time Monitor button.**

   The Real-time Monitor Options window appears:



3. **In the Direction field, select *Incoming and Outgoing Files*.**

   Files being copied *to* the server and files being opened for writing on the server are *incoming*. Incoming files are scanned after the file is closed.

   Files being copied *from* the server and files that are being executed from the server are *outgoing*. Outgoing files are scanned when the file is opened. If the file is found to be infected, you will be denied access to it.

   Other setting choices are *Incoming Files*, *Outgoing Files*, or *Disable*.

Scanning action

4. You control what happens to an infected file in the *Action Upon Virus Detection* field.

- Because you want to decide whether or not a file is cured on an individual basis, you choose the *Broadcast - No Action* option.
- If you prefer that an infected file be deleted automatically, choose *Delete File*.
- *Copy and Cure* makes a copy of the infected file and moves it to the INOCULAN/VIRUS directory before curing the file. InocuLAN removes viruses from infected files and restores the files to their original state. If the file cannot be cured, it will be renamed with an AVB extension (refer to 'Rename File' below). Even if InocuLAN cures the file, we recommend you delete the infected file and then restore the original file from a backup or the product installation disks.
- *Rename File* renames infected files by giving them an AVB extension. AVB files will not be scanned by InocuLAN. Infected files with the same name will be given incremental extensions in the form AV#, for example: FILE.AV0, FILE.AV1, etc.
- *Move File* moves an infected file from its current directory to the INOCULAN\VIRUS directory.
- *Purge File* deletes an infected file so that it cannot be recovered.
- *Rename and Move File* renames infected files by giving them an AVB extension and then moving them to the INOCULAN\VIRUS directory.

Whenever an action is taken, InocuLAN sends messages via Broadcast, Microsoft Mail, Microsoft Exchange, SNMP, Trouble Ticket, and Pager, if they have been set up in Alert. The message also appears in the Scanning Log and the Windows NT Event Log.

Scan Type

5. The level of scanning is set in the *Scan Type* field.

Because you want files to be scanned completely, choose *Secure Scan*. *Fast Scan*, which will run more quickly than Secure Scan, checks only the beginning and end of each data file, the place where a virus is most likely to hide. Fast Scan will improve scanning efficiency when processing large groups of data files, *but it is possible for a file to have a virus that will be missed by Fast Scan*.

If you suspect you have a virus but Secure Scan is not detecting one, you can use the *Reviewer Scan* option. The Reviewer Scan can also detect viruses that are inactive or have been deliberately modified, such as in a virus testing laboratory. Note that in unique circumstances, Reviewer Scan can generate a false alarm. Therefore, if you are using Reviewer Scan as your standard scanning option, you should use the Report Only option.

Floppy disk protection

6. Because floppy diskettes are the most common source of virus infections, we want to protect R&D DOMAIN from infected diskettes. Under Protected Areas, click *Protect Floppy Drives*.

As soon as a floppy diskette is accessed on any of the domain machines, InocuLAN scans the boot sector, preventing the spread of dangerous boot viruses. When a file is opened or copied from the floppy, InocuLAN scans it before it moves to the hard drive.

CD-ROM Protection

7. Because you will want to protect your environment from viruses when you download data or access data on CD's, you can now prevent viruses from being copied onto your machine.

Click on Protect CD-ROM Drive to enable this feature.

Server-to-Server protection

8. The users of R&D DOMAIN often copy files from one server to another.

By selecting *Protect Network Drives,* InocuLAN will scan all files moving between mapped drives, even if no file passes through the hard drive of the local machine.

Allow Fast Backup

9. The servers in R&D DOMAIN are backed up to tape each night.

Normally, the Real-time Monitor would scan each file as it was being copied to tape, thereby slowing the backup. However, since you scan the servers before the backup, you don't want to repeat the scanning during the backup. Click *Allow Fast Backup* to copy files to tape without virus scanning. InocuLAN will only skip files being opened by backup software. (Note that Cheyenne's ARCserve backup product integrates intelligently with InocuLAN, resulting in far less performance degradation than other backup products.)

Virus Wall

10. R&D DOMAIN supports hundreds of users.

Not all of them have anti-virus protection on their workstations, and some that do turn it off. This creates a very dangerous hole in your network security: infected files can be copied from a workstation to a server. By selecting *Virus-wall Incoming Mode*, InocuLAN will stop any infected file from being copied to a server and replacing the clean version of the file, thereby keeping enterprise security intact.

NOTE: InocuLAN currently protects.EXE,.COM,.DOC,.DOT, and.XLS files of less than 2MB in size for performance reasons.

Virus Source Tracking

11. It is important for the administrator to know who has tried to copy an infected file to R&D DOMAIN.

When *Report User Name* is selected, InocuLAN will report the name of the user trying to pass the virus. That person can then be contacted, and the virus deleted from their local machine.

Virus Quarantine

12. Because no network is perfect, and because end-users behave unpredictably, InocuLAN provides an exceptional level of protection through its virus *Quarantine* capability.

If Quarantine is activated, a user who attempts to move an infected file onto a server, or to execute an infected file at the server console, will be blocked from any further access to the server for the length of time stipulated in the *Quarantine Time* field. Quarantine ensures that the virus doesn't have a chance to spread before the infected workstation can be cleaned.

The names of quarantined users are found under the Quarantine tab in the Real-time Monitor Options screen. The administrator can grant the quarantined users access again by removing their name from the Quarantine screen.

NOTE: The Administrator account on the Windows NT machine cannot be quarantined. However, users with administrator rights can and will be quarantined.

Selecting files to scan

12. Now that the scanning options are set, you have to select the types of files you will scan.

Click on the Files tab.

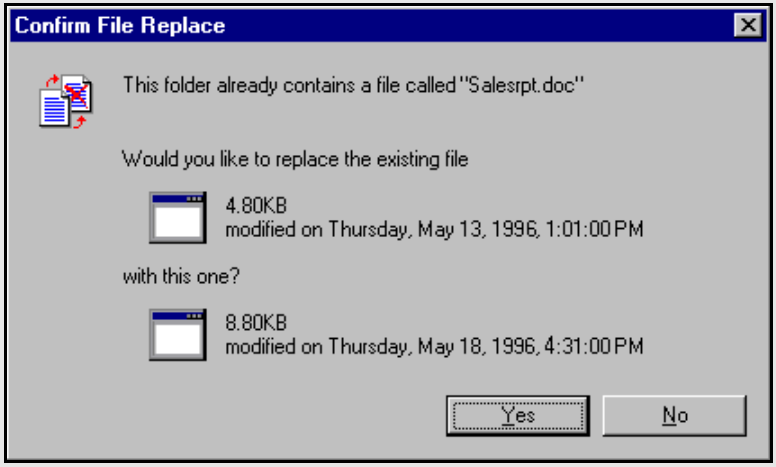
More about Quarantine and Virus Wall: A Test Scenario

To better understand the unique capabilities of the Quarantine and Virus Wall options, we will illustrate a test example.

In this scenario, we assume that user PeterE copied the file SALESRPT.DOC from the server to work with the file. Unfortunately, PeterE never scans his workstation for viruses, even though he has an anti-virus program. This resulted in the SALESRPT.DOC file becoming infected. PeterE will now attempt to copy the newly infected file back to the server. In an enterprise that didn't have InocuLAN's unique protection, the original SALESRPT.DOC file would be replaced with the infected version. Now the virus would be on the server, and the important data in SALESRPT.DOC would be at risk. Even worse, many people work with SALESRPT.DOC, so within a week dozens of people might have the virus.

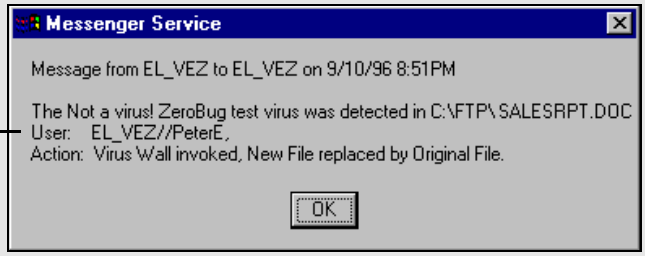
A recipe for enterprise disaster? Not if InocuLAN is up and running. Following are actual screens shots of this test scenario.

1. First, PeterE starts to copy the file back to the server. His machine asks him if he would like to replace the current file with the new version. Of course, he answers Yes. Without InocuLAN, the damage would already be done.



2. Fortunately, InocuLAN is running. Within seconds, the following appears on the NT Server:

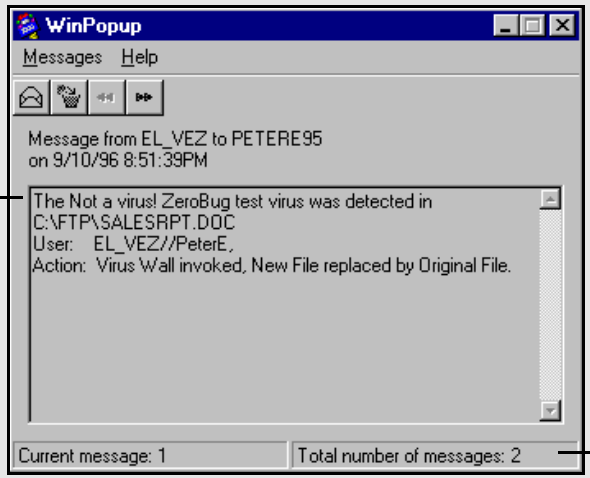
The administrator clearly sees who is trying to send a virus.



Virus Wall stops the infected file from overwriting the good file, and the important data in SALESRPT.DOC is safe, as is the server.

3. Meanwhile, on PeterE's machine, the following appears:

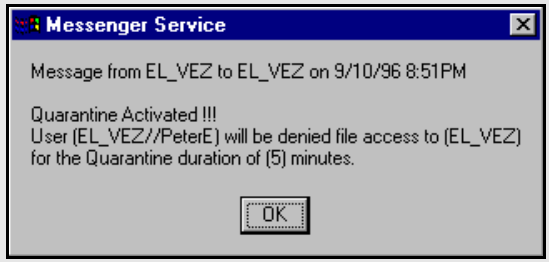
PeterE is informed that a virus was in his file, and that the Virus Wall has protected the server.



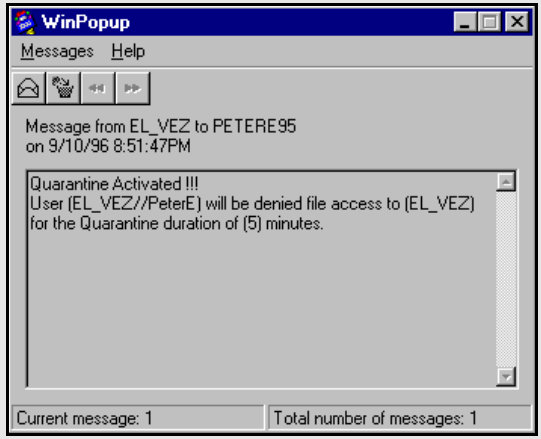
WinPopup shows a second message is waiting.

To receive messages from the NT server, the Windows 95 machine is running WinPopup. To run WinPopup, open the Run box and enter `Winpopup`. You may want to add Winpopup to your Startup group if you are using Quarantine. (Winpopup will also work on Windows 3.x workstations.)

4. After the administrator clicks OK on the first message, a second informs him that PeterE will be blocked from the EL_VEZ server for five minutes:

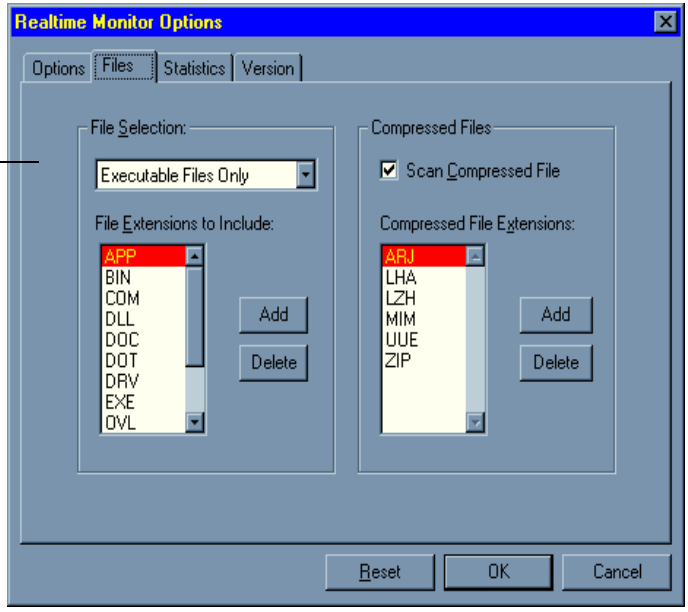


5. At the same time, when PeterE reads his second WinPopup message, he learns that he has been quarantined for five minutes.



The end result? The administrator knows that PeterE has a virus on his machine, and he can take action to remove it. PeterE knows that he has a virus, and he knows precisely how long he will be blocked from the server. And most importantly, the server has not been infected, and the original SALESRPT.DOC file is safe. The enterprise is secure.

Important! Because Quarantine blocks server access based on user name, any user named PeterE would have been quarantined in the above scenario. This is particularly important if a network has many people sharing the same user name, such as GUEST. All users names GUEST would be quarantined if one user tried to copy an infected file.



InocuLAN can scan all files, or you can include or exclude selected file types. You can also add and/or delete file types from the default list.

13. Choose *Scan Compressed File* for InocuLAN to scan compressed files.

By default, InocuLAN scans files of the ZIP and ARJ format, as well as LHA, LZH, MIME, UUEncoded, and Microsoft compressed files. These files end with an underscore, such as: START.EX_. To add other file types, click the Add button.

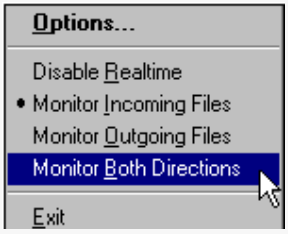
14. Click OK for your all options to take effect. Real-time scanning begins immediately.

With all of InocuLAN's Real-time scanning options now enabled, the R&D DOMAIN servers are thoroughly protected from all new viruses entering the network.

However, there may have been viruses present on the network before InocuLAN's Real-time scanning was turned on. To ensure that the network is clean, a full domain scan should be run. Instructions for doing so follow.

Windows NT 4.0 Enhancement - Real-time Quick Access Monitor

If you are using Windows NT 4.0, you can access the Real-time Monitor through the system tray. If you chose to install the Quick Access Monitor during setup, the icon will automatically appear in the system tray. To start it manually, click the Start button, then Programs, InocuLAN for Windows NT, and InocuLAN Real-time Monitor.



Double-clicking on the Quick Access Monitor icon (at right) will open the Real-time Monitor's Options screen. Right-clicking on it will also allow you to open the Options screen, alter the direction of files being scanned or disable the monitor, as

Scheduling the Domain Scan

With the domain set up and real-time scanning in place, the next task is to schedule a domain scan job.

1. Click the Add/Re-Schedule a Scan Job button.

Information about what and when to scan is entered on the Targets/Schedules tab:

The asterisk '*' indicates that all drives will be scanned. To scan only selected drives, click the Browse button and choose the drives you want to scan.

Check here to scan all subdirectories beneath the source drive.

You can scan your InocuLAN machines as they start up by clicking here. This will insure a clean machine before work starts.

To run a scan at regular intervals, set the repeat time here. Leave at zero to scan only once. This shows a scan set to run every day.

Indicate when the scan should start. The default is the current date and time.

2. Because the servers on the R&D DOMAIN are heavily used, you don't want the scanning process to utilize too much CPU power.

Set the *CPU Usage Level* to a relatively low level, such as 3. A less busy domain could be set at a higher level, up to 10, which gives full CPU power to the scanning engine. This value is best determined through usage.

3. **One directory in the domain, D:\ARCHIVE, contains a large number of compressed archive files.**

   This directory takes a long time to scan. However, since all your archive files are scanned before being compressed, you know they are virus-free.

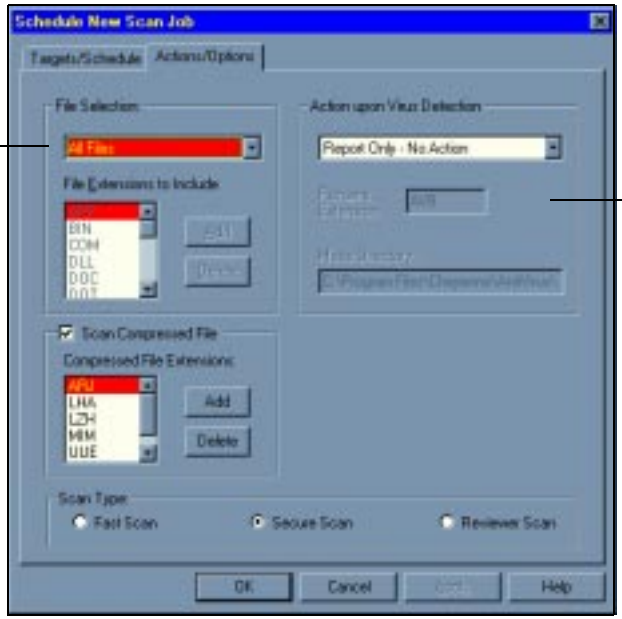
   You can skip this directory by adding it to the *Exclude Selected Directories and Files from Scan* field.

Setting scan actions and options

4. Now you must select which scanning options to use, and what to do if a virus is found.

Click the Action/Options tab on the Schedule New Scan Job screen.

InocuLAN can scan all files, or you can include or exclude selected file types. You can also add and/or delete file types from the default list.



Rename of the file extension(s) will occur if Cure fails

5. Select the options you want to include with the scanning job.

Choose *Scan Compressed File* for InocuLAN to scan compressed files.

By default, InocuLAN scans files of the ZIP and ARJ format, as well as LHA, LZH, MIME, UUEncoded, and Microsoft compressed files. These files end with an underscore, such as: START.EX_. To add other file types, click the add button.

Scanning action

6. You control what happens to an infected file in the *Action Upon Virus Detection* field.

- Because you want to decide whether or not a file is cured on an individual basis, you choose the *Broadcast - No Action* option.
- If you prefer that an infected file be deleted automatically, choose *Delete File*.
- *Cure Files* removes viruses from infected files and restores the files to their original state. If the file cannot be cured, it will be renamed with an AVB extension (refer to 'Rename File' below). Even if InocuLAN cures the file, we recommend you delete the infected file and then restore the original file from a backup or the product installation disks.
- *Rename File* renames infected files by giving them an AVB extension. AVB files will not be scanned by InocuLAN. Infected files with the same name will be given incremental extensions in the form AV#, for example: FILE.AV0, FILE.AV1, etc.
- *Move File* moves an infected file from its current directory to the INOCULAN\VIRUS directory.
- *Purge File* deletes an infected file so that it cannot be recovered.
- *Rename and Move File* renames infected files by giving them an AVB extension and then moving them to the INOCULAN\VIRUS directory.

Whenever an action is taken, InocuLAN sends messages via Broadcast, Microsoft Mail, Microsoft Exchange, SNMP, Trouble Ticket, and Pager, if they have been set up in Alert. The message also appears in the Scanning Log and the Windows NT Event Log.

Scan Type

7. The level of scanning is set in the *Scan Type* field.

Because you want to ensure that files are scanned in their entirety, you choose *Secure Scan*. *Fast Scan*, which will run quicker than Secure Scan, checks only the beginning and end of each data file, the place where a

virus is most likely to hide. Fast Scan will improve scanning efficiency when processing large groups of data files, *but it is possible for a file to have a virus that will be missed by Fast Scan.*

If you suspect you have a virus but Secure Scan is not detecting one, you can use the *Reviewer Scan* option. The Reviewer Scan can also detect viruses that are inactive or have been deliberately modified, such as in a virus testing laboratory. Note that in unique circumstances, Reviewer Scan can generate a false alarm. Therefore, if you are using Reviewer Scan as your standard scanning option, you should use the Report Only option.

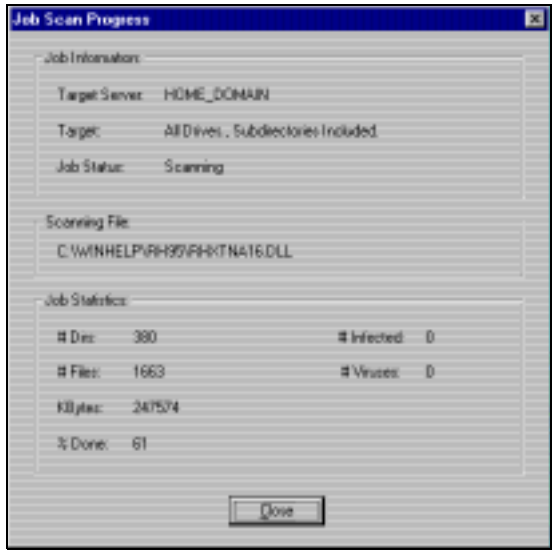
8. Click OK to apply your domain scanning settings.

Starting the domain scan and checking scan progress

After clicking OK on the Schedule New Scan Job screen, the scan is set to start based on your configuration. The *Job Status* field in the Domain Manager window will tell you if a job is scheduled to begin, if it is currently scanning, or if the scan has completed.

If a scan is shown as *Active*, you can view the scan progress by clicking on that job to bring up the Scan Progress window:

The progress of the scan job is dynamically displayed in the window, along with an indication of how much of the scan has completed.



NOTE: You should not leave the Scan Progress window open for the length of the scan because it will slow down the scanning operation.

Viewing the scan results

After your scan job is complete, you can view the results of your scan as follows:

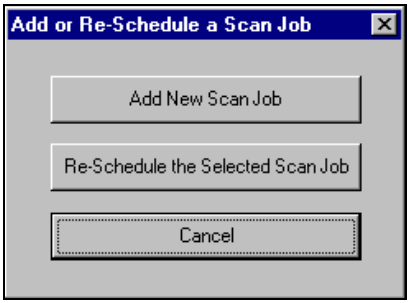
1. **Highlight a domain and click the Scan Job and Log View icon.**

2. **In the Job Log window, double-click a log to access the scanning record information.**

Modifying a Scan Job

Once you have scheduled a new scan job, it can be modified to fit your changing requirements.

1. **Highlight the scheduled job in the Job Queue Screen.**
2. **Click the Add/Re-Schedule a Scan Job button.**
3. **The Add or Re-schedule a Scan Job screen is displayed:**



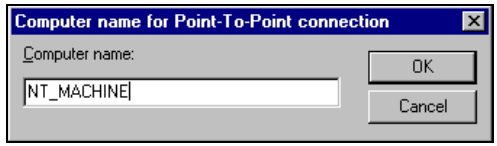
4. **Click the *Re-Schedule the Selected scan job* button.**
   The Modify/re-schedule Scan Job dialog box opens.
5. **Make the changes in either the Targets/Schedule screen or the Actions/Options screen.**
6. **Click OK when done to apply the changes.**

Point-to-Point management

InocuLAN servers periodically send broadcasts, allowing the InocuLAN browser to locate them. However, your network may be configured to filter such messages, and some InocuLAN machines may not appear in the browser. If this is the case, you can attach to those machines directly using point-to-point management.

To configure Point-To-Point management:

1. **Click the *Point -To- Point* button in the Domain Manager window. This will open the computer name**



entry window:

2. **Enter the name of the InocuLAN server and click OK.**

   The server will appear in the browser under the Point-to-Point heading.

NOTE: Machines located by point-to-point management cannot be included as part of an InocuLAN domain and must be administered separately.

NetWare Domain Management

InocuLAN 4 for Windows NT gives you the ability to manage your InocuLAN for NetWare domains through the Windows NT console.

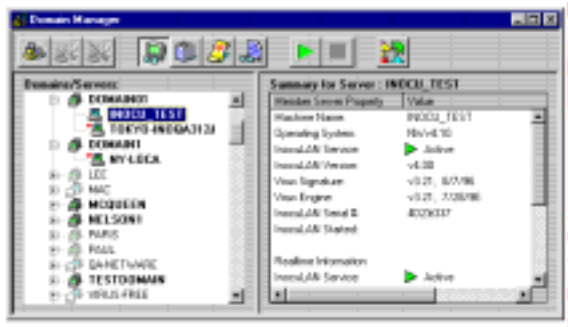
To manage your InocuLAN for NetWare domains:

1. **Click the Domain Manager for NetWare button on the Quick Access screen.**

2. **The Select InocuLAN NetWare Server screen will appear. All available NetWare servers will show in the list. Choose any server that has InocuLAN for NetWare running on it.**

Click OK to continue.

3. **The InocuLAN for NetWare Domain Manager will appear. This screen allows full InocuLAN domain management.**



NOTE: For details on InocuLAN for NetWare management, consult the *InocuLAN for NetWare Supervisor Guide*.

Using the Local Scanner

The Local Scanner scans files on your local machine, on mapped drives, and on networked machines.

Local Scanner vs. domain management

InocuLAN's domain management provides extensive protection for the NT enterprise. However, certain situations are more easily and effectively handled by the Local Scanner. For instance:

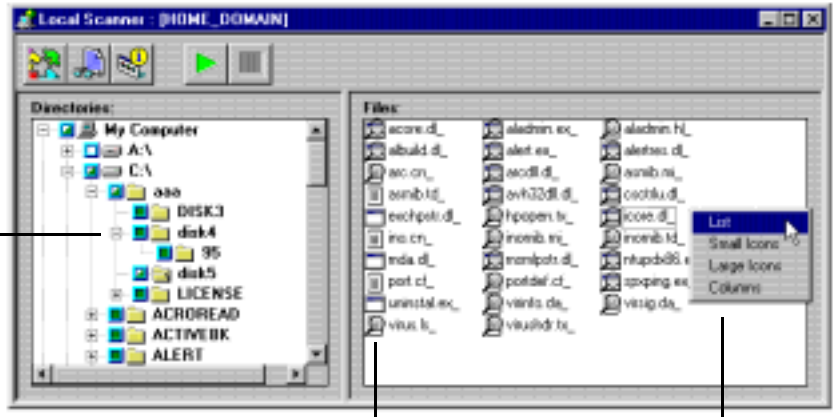
- Scanning a server that is not part of a network.
- Scanning a particular directory or file.
- Scanning a floppy diskette or CD.

How to use the Local Scanner

Follow the instructions below to use the Local Scanner.

1. Click the Local Scanner button to open the scanner:

The Explorer-style browser lets you select what to scan, right down to the individual file level.



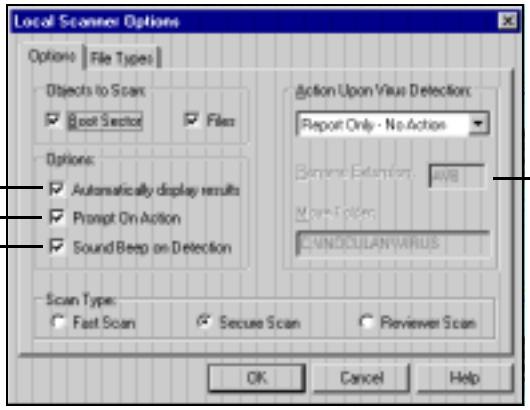
The magnifying glass icon indicates that a file will be scanned. Click a file to change the setting, or highlight a group of files and right-click to bring up the select/deselect button.

Right-clicking in the Files window lets you change the way files are viewed, using the same options found in the Windows Explorer.

2. Select the drives, directories and/or files you want to scan.

3. Set the scanning options by clicking on the Options button.

The Local Scanner Options dialog box will appear:



Click here to see scan results as soon as the scan is finished. Otherwise, you can view results in the Scan Log.

Click here to be notified before InocuLAN takes action on infected files.

Check here for InocuLAN to beep when a virus is detected.

File will be renamed if Cure Action fails.

4. Because we want to make all scans are as secure as possible, we will choose both *Boot Sector* and *Files* in the Objects to Scan field. If you suspected a floppy diskette had a boot sector virus, you might deselect *Files* to speed up the scanning process.

Scanning actions

5. You control what happens to an infected file in the *Action Upon Virus Detection* field.

- Because you want to decide whether or not a file is cured on an individual basis, you choose the *Broadcast - No Action* option.
- If you prefer that an infected file be deleted automatically, choose *Delete File*.
- *Cure Files* removes viruses from infected files and restores the files to their original state. If the file cannot be cured, it will be renamed with an AVB extension (refer to 'Rename File' below). Even if InocuLAN cures the file, we recommend you

delete the infected file and then restore the original file from a backup or the product installation disks.

- *Rename File* renames infected files by giving them an AVB extension. AVB files will not be scanned by InocuLAN. Infected files with the same name will be given incremental extensions in the form AV#, for example: FILE.AV0, FILE.AV1, etc.
- *Move File* moves an infected file from its current directory to the INOCULAN\VIRUS directory.
- *Purge File* deletes an infected file so that it cannot be recovered.
- *Rename and Move File* renames infected files by giving them an AVB extension and then moving them to the INOCULAN\VIRUS directory.

Whenever an action is taken, InocuLAN sends messages via Broadcast, Microsoft Mail, Microsoft Exchange, SNMP, Trouble Ticket, and Pager, if they have been set up in Alert. The message also appears in the Scanning Log and the Windows NT Event Log.

Scan Type

6. The level of scanning is set in the *Scan Type* field.

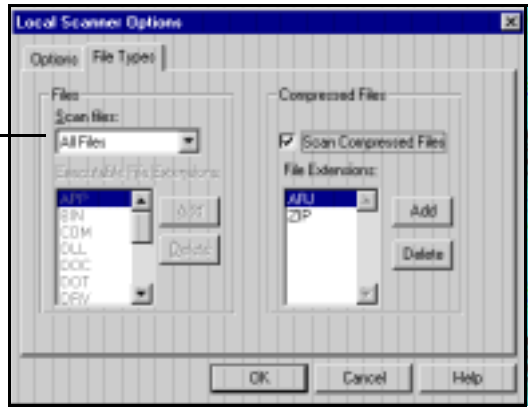
Because you want to ensure that files are scanned in their entirety, you choose *Secure Scan. Fast Scan,* which will run quicker than Secure Scan, checks only the beginning and end of each data file, the place where a virus is most likely to hide. Fast Scan will improve scanning efficiency when processing large groups of data files, *but it is possible for a file to have a virus that will be missed by Fast Scan.*

If you suspect you have a virus but Secure Scan is not detecting one, you can use the *Reviewer Scan* option. The Reviewer Scan can also detect viruses that are inactive or have been deliberately modified, such as in a virus testing laboratory. Note that in unique circumstances, Reviewer Scan can generate a false alarm. Therefore, if you are using Reviewer Scan as

your standard scanning option, you should use the Report Only option.

Selecting files to scan

7. Now that the scanning options are set, you have to select the types of files you will scan. Click on the Files tab.



InocuLAN can scan all files, or you can include or exclude selected file types. You can also add and/or delete file types from the default list.

Scan Compressed file

8. Choose *Scan Compressed File* for InocuLAN to scan compressed files.

By default, InocuLAN scans files of the ZIP and ARJ format, as well as LHA,LZH, MIME, UUEncoded, and Microsoft compressed files. These files end with an underscore, such as: START.EX_. To add other file types, click the add button.

9. Click OK to accept the settings.

10. Click the Start/Continue Scanning Drive button. The scan begins immediately. Scanning progress can be seen in the Local Scanner window.

11. When the scan is completed, the Virus Scan Results window will display scanning information, including the name and location of any viruses that were found.

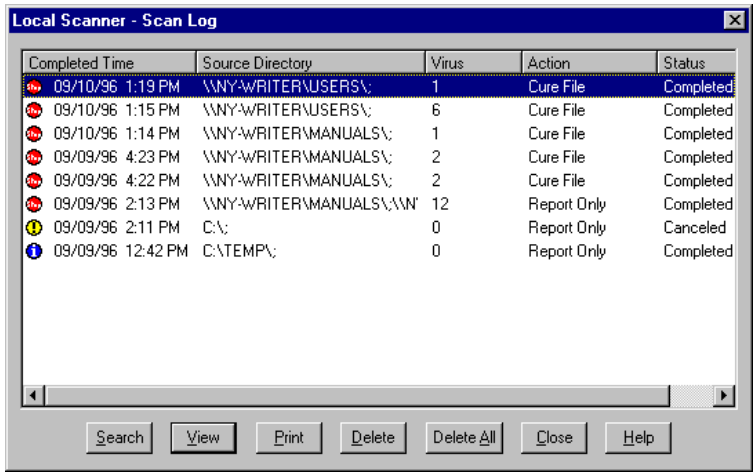
NOTE: If you use the Local Scanner to scan a mapped drive on a machine that is running InocuLAN's Real-time Monitor, the scanner may not be able to detect all viruses. This is because as the scanner attempts to access an infected file for scanning, the Real-time Monitor will catch the virus and block access to the file. However, if your Real-time Monitor is configured to only scan certain file types (such as .exe), the Local Scanner will detect other types of files that are infected.

Checking the results of your scan

If you have the option *Automatically Display Results* selected, the results of your scan will appear on the screen when the scan is completed.

If you do not have this option selected, or if you want to view the results at a later time, follow the instructions below:

1. **Click the Scan Log button. The Local Scanner Scan Log appears:**

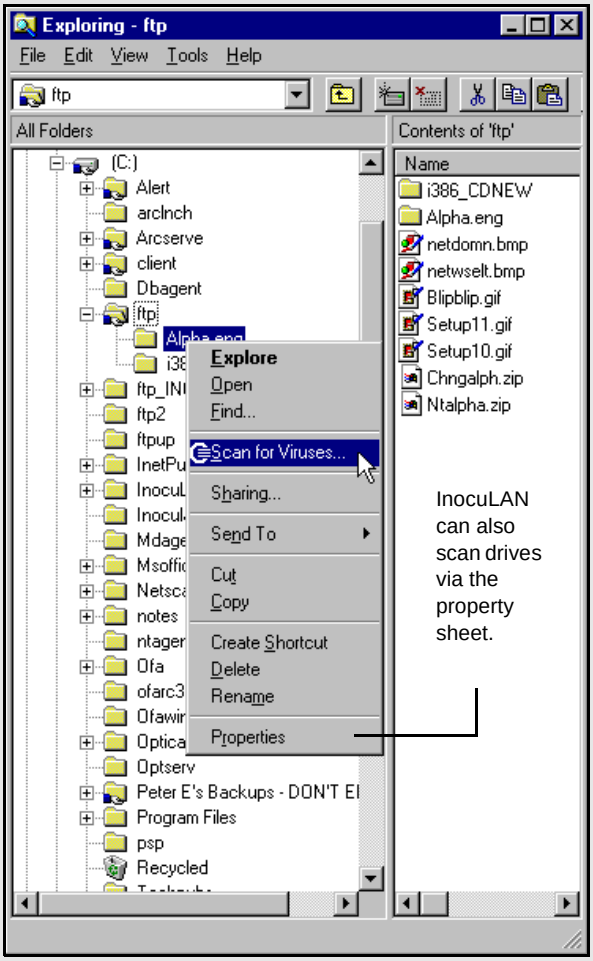


2. **Highlight the job you want to find out more information about.**

3. **Click View or double-click on the job to view details of the scanning job.**

Windows NT 4.0 Enhancement - Local Scanning shell extensions

If you are using Windows NT 4.0, you can quickly scan a directory or file by using InocuLAN's shell extensions.



To use the shell extensions, locate a directory or file in My Computer or the Windows Explorer. Right-click on the directory or file and select *Scan for Viruses...*, as shown at the left.

This will open the InocuLAN shell scanner. The shell scanner uses the same scanning engine and has the same functionality as the Local Scanner. To set the scanning options, click *Advanced*. (For information on scanning options, see "How to use the Local Scanner" on page 2-29.) Click Start to begin the scan. Scan progress will be shown by a moving progress bar. Scan reports are sent to the Local Scanner Scanning Log and can be reviewed there.

Internet-Enabled Download Protection

InocuLAN 4 for Windows NT protects NT servers from a rapidly-growing source of infection: Internet downloads.

Protection is automatic. If you selected Netscape Navigator and/or Microsoft Internet Explorer during the Internet Options portion of the InocuLAN installation, InocuLAN is already configured to work with your browser.

When you start a web page or FTP download with your browser, InocuLAN will start its Internet helper application to check the file for viruses while the download is taking place.

If no virus is detected, the Save box will appear and you can proceed with your download. If a virus is detected, the file will be moved to the Temp directory where it can be cured.

General suggestions

In addition to all of InocuLAN's features, we offer the following general suggestions to help keep your network virus-free:

- Set all of your executable files as Read Only files. Since a virus has the access rights of the user, making these files Read Only will reduce the chance of executable files becoming infected with viruses by non-administrator users.
- Be careful with administrator privileges. Logging in as an administrator or having administrator-equivalent privileges gives you access to the file server's directory structure. This means you can infect the

entire directory structure if your workstation is infected with a virus. Therefore, you should not log in as a administrator unless you actually need administrator privileges to perform a task.

- Do not grant users “read” or “open” rights to other users’ directories. Viruses can be spread if a user executes an infected program or copies an infected file from another directory.
- Use InocuLAN to scan floppy diskettes for viruses before copying any files from them.
- Back up your network after you successfully scan the network for viruses. This way, if InocuLAN detects a file with a virus that cannot be cured, you can restore a backed up, virus free version of that file.

3

C h a p t e r

CONFIGURING SERVICES, LOGS AND BROADCASTS

InocuLAN's Service Manager lets you fine-tune your InocuLAN enterprise through configuration of Services, Logs and network Broadcasts.

In this chapter, you will learn:

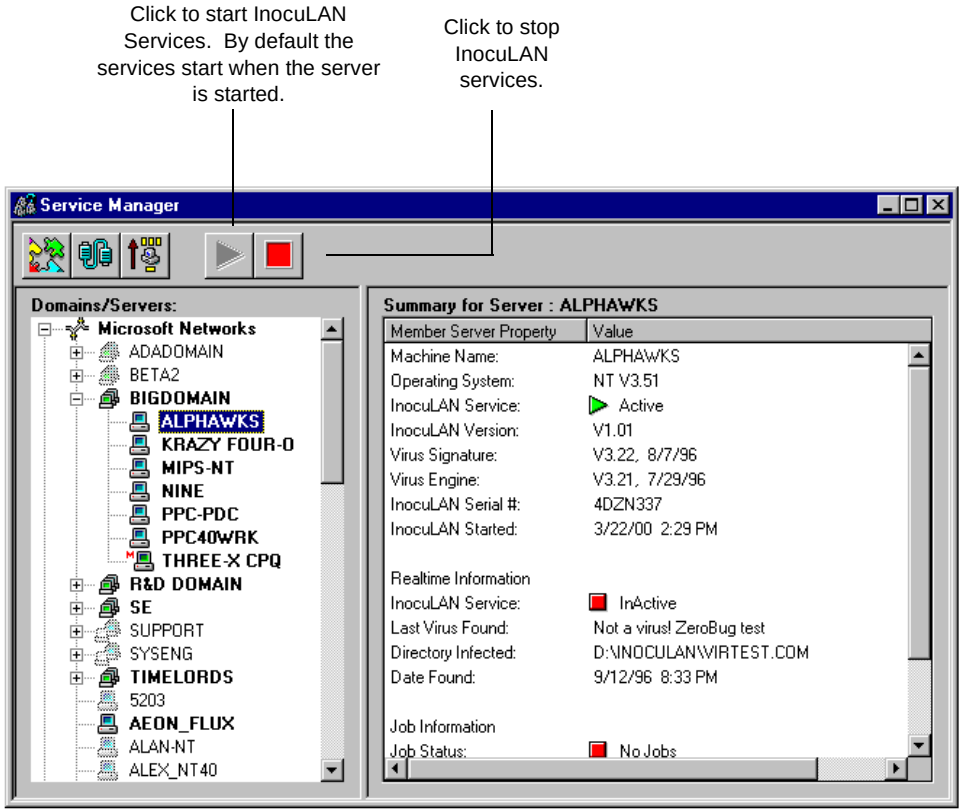
The Service Manager

InocuLAN's Service Manager allows you to start, stop and configure the InocuLAN service parameters.

Accessing the Service Manager

1. **In the Quick Access Box, click the Service Manager button.**

   The Service Manager Summary screen appears:



Configuring InocuLAN's Services

This section explains how to configure InocuLAN's services.

1. Click the Configuration button.

The Service Configuration Screen appears:

Automatic Startup — This option will automatically start the background services when the Windows NT machine is booted up.

Manual Startup — This option requires you to start up the InocuLAN Services manually via the Service Manager screen or the Windows NT Control Panel.

Completed Job Hold Time — Enter the number of days a finished job should remain in the Job Queue.

Active Server Time-out

Indicate how long InocuLAN should wait before considering a server inactive if the server has not sent any messages.

This feature works in conjunction with the Heartbeat Update Interval, explained on page 3-15.

NOTE: The longer the time-out value, the longer it will take for the service to time-out an InocuLAN server. All InocuLAN machines should be configured with the identical value. If the values are different, some machines will appear to be on-line while some appear to be off-line.

Configuring the Event Log

This section explains how to configure the InocuLAN Event Log.

1. In the Service Configuration screen, click the Event Log tab.

The Event Log Configuration screen appears:

Maximum Messages — Indicate the maximum number of messages that should remain in the Event Log.

Purge Records Older than — Indicate how long you want to keep an event in the log.

Message filters — You can select the type(s) of message(s) that should be stored in the Event Log.

- *Critical Message:* This is the highest level message. It requires your immediate attention once logged. This message could

mean there is a virus detected, or there is a problem with the service. This is selected by default.

- *Warning Message:* The second priority message tells you if InocuLAN skips a file, and other non-critical information.
- *Informational Message:* This will tell you if the service has started or stopped and if no viruses have been found.

Configuring the Scan Log

This section explains how to configure the InocuLAN Scan Log.

1. In the Service Configuration Screen, click the Scan Log tab.

The Scan Log Configuration screen appears:

This option cannot be deselected.

Maximum Messages — Indicate the maximum number of messages that should remain in the Scan Log.

Purge Records older than — Indicate how long you want to keep a scan record in the log.

Message Filters — You can select the type(s) of message(s) that should be stored in the Scan Log.

- *Critical Message:* A critical message will alert you when a virus is detected.
- *Warning Message:* A warning message will tell you when a job was cancelled.

- *Informational Message:* An information message will tell you when a job is completed with no virus found.

Configuring the Virus Directory Purge

This section explains how to configure the InocuLAN Virus Directory Purge.

1. **In the Service Configuration screen, click the Virus Directory tab.**

   The Virus Directory Configuration screen appears:

Perform Virus Directory Cleanup

Check this box to schedule a full cleanup of the Virus Directory.

Purge files older than...

The number you enter represents the age of the files to be purged. For example, if you enter the number 360, any files that remain in the Virus Directory *longer* than 360 days will be purged on Day 361.

Configuring Broadcast services

Applications often use a network broadcast to ‘advertise’ themselves to other computers on the network.

InocuLAN may be configured to use the Mailslots protocol, TCP/IP protocol, or a combination of both. InocuLAN broadcasts include status changes, signature versions, engine versions, real-time and scheduled job status changes, and the OS version running on the server.

This section explains how to configure the InocuLAN broadcasts.

Hands-free configuration

InocuLAN 4 for Windows NT features a powerful network Auto Discover feature. InocuLAN machines can typically find each other on the network right out of the box, with no administrative intervention.

However, there are some instances when it may be necessary or desirable to manually alter some of the default settings. Possible scenarios that may require configuring include:

- Some of the InocuLAN machines cannot see each other. This may be due to routers blocking the InocuLAN broadcasts, or by machines being located on different IP subnets.
- You may wish to reduce broadcast traffic on your network. InocuLAN allows you to adjust the broadcast frequency to achieve the proper balance between accurate machine reporting and network throughput.

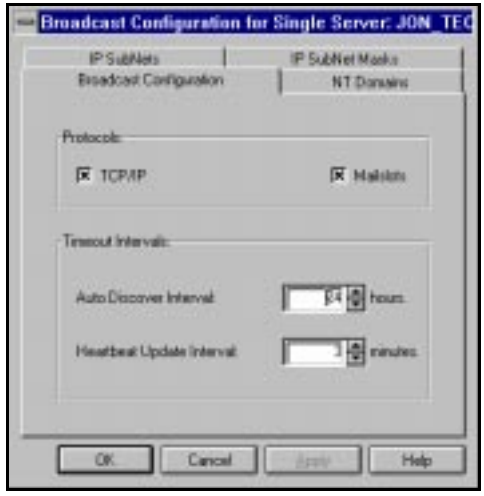
NOTE: Manual configuration of the InocuLAN network should be reserved for special, specific needs. It is recommend that the default values be tried initially. Because InocuLAN allows for very precise broadcast configuration, *only a network administrator should attempt to manually configure the software.*

Configuring Broadcasts

InocuLAN's network broadcasts can be configured as shown below.

1. Click the InocuLAN Service Configuration button.

The Broadcast Configuration screen appears:



Protocols

Mailslots and TCP/IP

Both settings are active by default. They allow InocuLAN to broadcast messages over both Mailslots (NT Domains) and TCP/IP (IP Networks) protocols. This setting is the most thorough, however it may cause network traffic.

Mailslots configures InocuLAN to broadcast its messages over the Mailslots protocol only. Choose this if you have a mixed environment, and are certain that Mailslots broadcasts will reach all destinations.

TCP/IP configures InocuLAN to broadcast its messages over the IP protocol only. Choose this if you have an IP only network.

Time-out Intervals

Auto Discover Interval

Auto Discover allows InocuLAN to search your network for Windows NT domains and IP subnets. In a dynamic network, it is important that InocuLAN maintain a record of the machines it broadcasts to. InocuLAN maintains this record in three tables:

- NT Domain table - Auto Discover adds new NT Domains to this table (DOMAIN.TBL). This allows InocuLAN to broadcast via Mailslots to all machines in the listed Domain.
- IP Mask table - This table contains the local IP Mask (IPMASK.TBL) by default. If your environment supports more than one mask, they must be entered manually and the InocuLAN Service re-started.
- IP Subnet table - Once updated, InocuLAN uses the NT Domain and IP Mask tables to discover/add new IP Subnets to the IP Subnet table (IPNET.TBL). This allows InocuLAN to broadcast via IP to all IP Subnets specified in the IP Subnet table.

Auto Discover adds NT domains and IP Subnets to these tables according to the hourly setting you choose.

NOTE: Please note that a zero (0) value disables Auto Discover.

Heartbeat Update Interval

This setting tells InocuLAN to broadcast a "Heartbeat," or reminder broadcast, updating its status to the other InocuLAN machines on the network. This ensures that the status of all InocuLAN machines is known. The default time is three minutes.

NOTE: All InocuLAN machines should have the same Heartbeat Update Interval setting. Otherwise conflicting messages may be sent.

The Heartbeat Update Interval is set in conjunction with the *Active Server Time-out* setting, which is always three times (3x) the value of the *Heartbeat Update.* For example, if the Heartbeat Update Interval is set to five minutes, the Active Server Timeout will be set to 15 minutes, three heartbeats per timeout. You need only set one value: no matter which you set, the other will automatically set itself to the correct corresponding value.

If a heartbeat is not received within the Active Server Timeout limit, the machine will be considered down/ inactive.

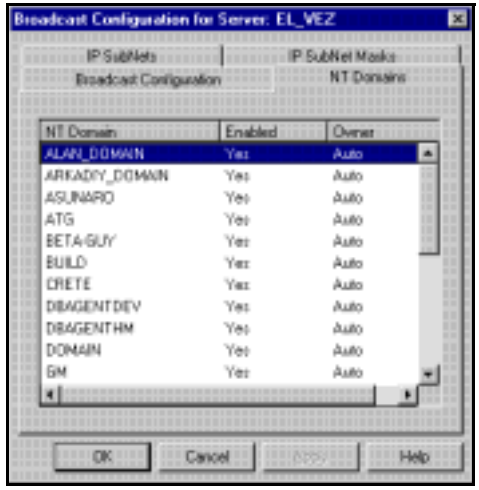
Configuring NT Domains

This section explains how to configure the NT Domains to which InocuLAN will be broadcasting.

For InocuLAN to broadcast to an NT domain, the *Mailslots* protocol must be enabled.

1. To configure NT domains, select the NT Domains tab:

All domains located by Auto Discover will appear in the list automatically.



Information entered here will be added to the NT Domain table.

Adding/deleting domains

To add a new domain, press *Insert* and type the new name in the dialog box. To delete an existing domain, highlight it, and press *Delete*.

Changing the status of an existing domain

You can *enable*, *disable*, or *change the name* of the selected domain by double-clicking it and entering the proper information in the dialog box.

Configuring TCP/IP Networks

This section explains how to configure the IP Subnets to which InocuLAN IP broadcasts go.

For InocuLAN to broadcast to an IP Subnet, the *TCP/IP* protocol must be enabled.

Adding/deleting IP Networks

To add a new IP Network (IP Net and the IP Mask), simply press *Insert*, and type the new number(s) in the dialog box. To delete an existing IP Network, highlight it and press *Delete.*

Changing the status of an existing IP Network

You can *enable*, *disable*, or *change the number(s)* of the selected IP Network by double-clicking it with the left mouse button and entering the proper information in the dialog box.

Configuring IP Network Masks

This section explains how to configure the IP Network Masks.

InocuLAN uses this information in the Auto Discovery of IP Subnets. (Refer to 'Timeout Intervals' on page 3-14 for more information on the Auto Discovery feature.)

Information entered here will be added to the IP Net table. The IP Net(s) entered will supersede data found via the Auto Discovery feature.

Adding/deleting IP Network Masks

To add a new IP Network Mask, simply press *Insert*, and type the new number in the dialog box. To delete an existing IP Network Mask, highlight it, and press *Delete*.

Changing the status of an existing IP Network mask

You can *enable*, *disable*, or *change the number* of the selected IP Network Mask by double-clicking it with the left mouse button and entering the proper information in the dialog box.

Troubleshooting the InocuLAN network

If InocuLAN cannot see all of the InocuLAN machines in your environment:

1. Check the NT Domain table. It should contain all of the NT Domains. If a Windows NT Domain is not listed, manually add it to the NT Domain table.

2. Check the IP Subnet table. It should contain all of the IP Subnets. If an IP Subnet is not listed, manually add it to the IP Subnet table.

3. Check the *Network Connections* box of the Windows NT 3.51 File Manager or the *Network Neighborhood* of Windows NT 4.0. If these do not contain the InocuLAN machine(s) you are looking for, re-check your Windows NT configuration.

4. In a mixed InocuLAN domain of version 1.01 and 4, the Master Server must be an InocuLAN 4 machine.

5. Check that the Heartbeat Intervals are the same on all of your InocuLAN machines.

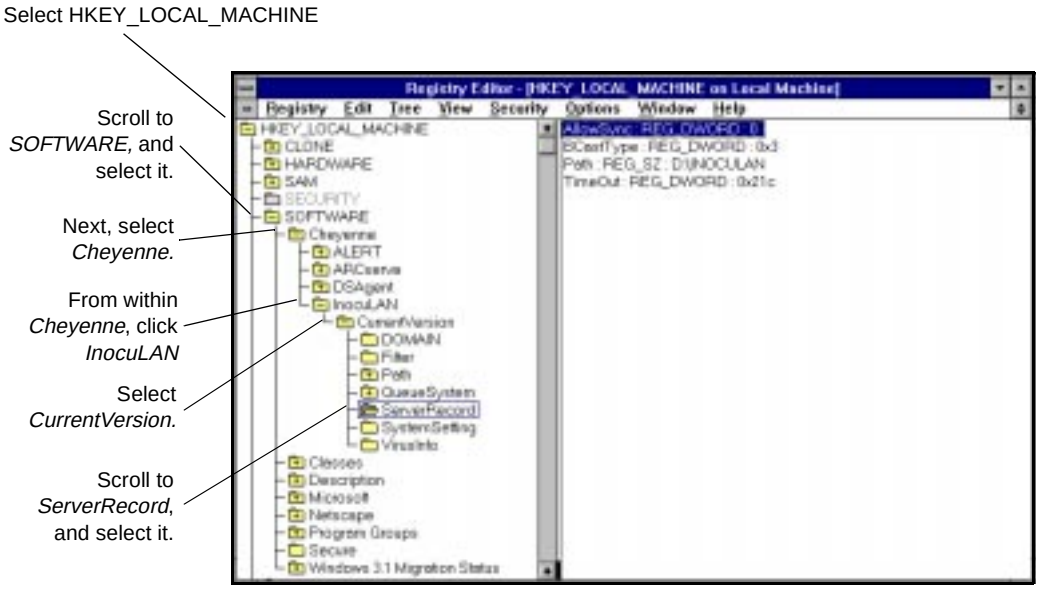
Synchronizing broadcast information

This feature allows an InocuLAN Administrator to update the Broadcast configuration of ALL InocuLAN machines on the network, based on the setting of one InocuLAN machine.

To synchronize InocuLAN broadcasts:

1. **Open the Windows NT Registry Editor.**
   In the Run dialog box, type the following command:
   `Regedt32`
2. **Click OK.**

The Registry Editor screen will appear. Follow the steps below:



3. **Once in the *ServerRecord* folder, highlight AllowSync: REG_DWORD.**

   Note that the default value = 0

4. **Click on *AllowSync: REG_DWORD: 0*. The DWord Editor dialog box will appear.**

5. **From within the DWord Editor, enter 1 in the Data column, and click OK.**

   The AllowSync: REG_DWORD value will now read: 0x1.

   This value activates the Synchronize feature.

6. **Close the Registry Editor, and return to the InocuLAN Service Manager screen.**

7. **From the InocuLAN Service Manager Menu, highlight *Service* and select *Synchronize.***

The Synchronize Broadcast information dialog box will appear:

The Source Server from which InocuLAN will be synchronizing all of the network InocuLAN computers.

Select the items you wish to synchronize.

NOTE: Please make sure that you are using the correct Source Server. The broadcast settings for all other InocuLAN computers will be based on this server!

8. **Select the items you wish to synchronize.**

9. **Click OK.**

Synchronizing may take a few minutes to complete.

AUTOMATIC DOWNLOAD, DISTRIBUTION AND UPDATE

InocuLAN's hands-free AutoDownload and distribution functions keep your network up-to-date with minimal user effort.

In this chapter, you will learn:

Automatic Signature Download, Distribution and Update

One of the most significant features of InocuLAN 4 for Windows NT is the ability to automatically download and distribute the latest signature files and software updates. InocuLAN includes a utility called AutoDownload which retrieves the latest files from the Cheyenne InocuLAN update site, either via FTP or via modem, and stores them in an InocuLAN sub-directory. InocuLAN will then distribute these files to other InocuLAN servers. The AVUPDATE program can also be used to update files on Windows 95, Windows 3.x and DOS workstations when they log in to servers running InocuLAN.

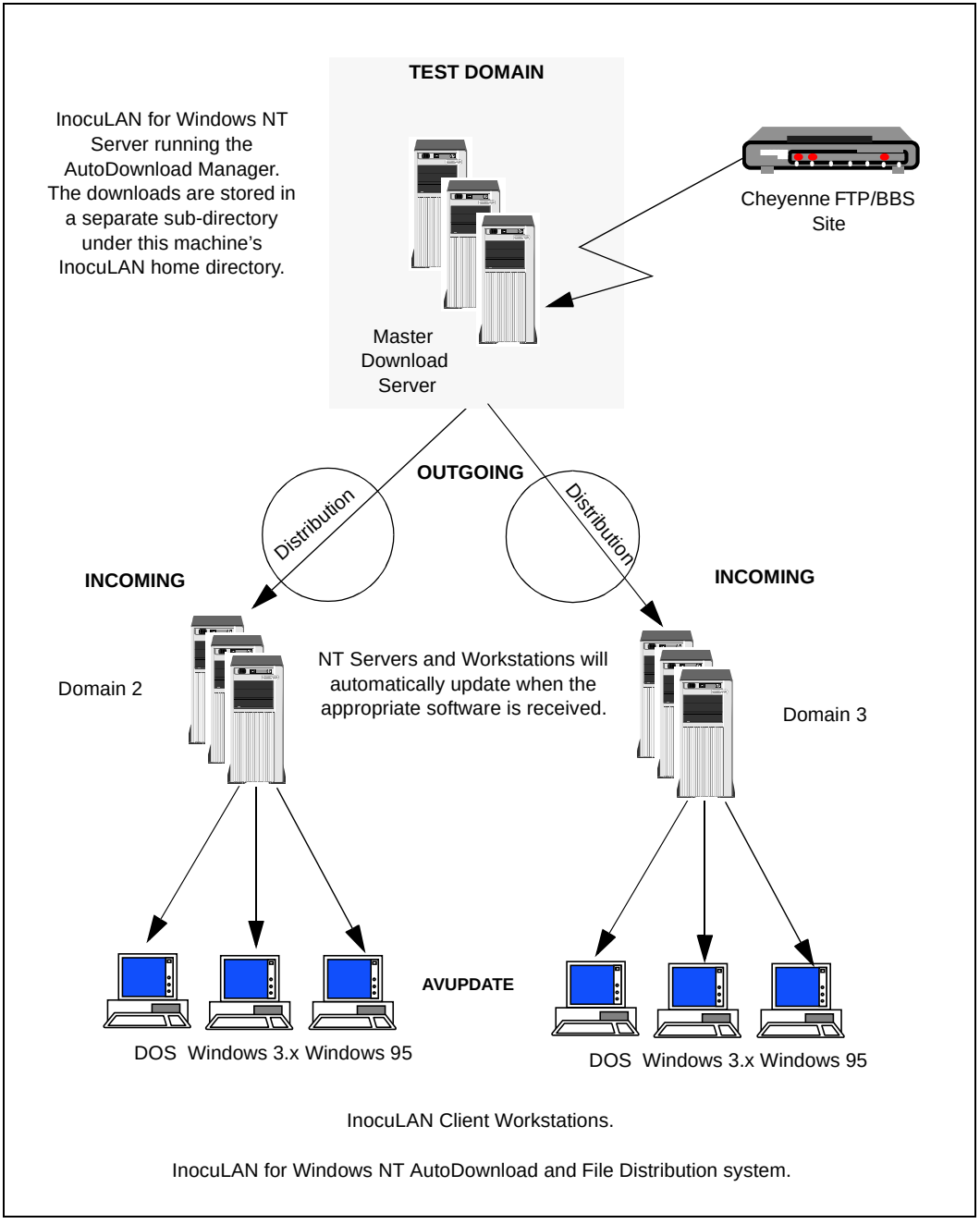
NOTE: To prevent you from overwriting the pre-configured AVUPDATE.INI files, when you download or install InocuLAN on your server(s), the AVUPDATE file is initially named AVUPDATE.INO. You can rename this file later.

The following outlines the sequence of events needed to update an InocuLAN network.

- AutoDownload retrieves the signature files and software updates and stores them in the AutoDownload directory (called **GBBSdata**).
- InocuLAN's Distribution function on the AutoDownload machine then copies the files from the GBBSdata directory into the InocuLAN distribution directory (called **Update**), where they will be made available to other InocuLAN machines. Distribution parameters are provided to

specify when to retrieve files, what platforms and languages to retrieve, and what server(s) to get them from.

- Other InocuLAN machines access the Update directory for files and update themselves based on pre-set parameters.
- Windows 95, Windows 3.x and DOS clients are updated when they log in to a Windows NT domain set up to run the AVUPDATE program from a login script. (Please see the Release Notes for details about AVUPDATE.)



InocuLAN Client Workstations.

InocuLAN for Windows NT AutoDownload and File Distribution system.

AutoDownload, Distribution and Update: A Scenario

AutoDownload and distribution is a very powerful feature of InocuLAN 4 for Windows NT. Once set up, the system will automatically download files, distribute them across the network, and update all InocuLAN machines, each step carefully controlled by InocuLAN's extensive feature set.

To best explain the concept and procedures of AutoDownload and distribution, the following pages will outline a sample distribution scenario.

The network in our scenario consists of the following:

- A test InocuLAN domain called R&D DOMAIN. This domain consists of a Master Server and three member servers.
- A full production network of InocuLAN machines.

Our AutoDownload and distribution plan has four distinct stages:

- Stage 1: To download the latest InocuLAN files from Cheyenne Software. Files will be downloaded by the Master Server on R&D DOMAIN.
- Stage 2: The Master Server will access the new files and update itself based on pre-set parameters. The Master Server will hold the files for three days before making them available to the other machines in R&D DOMAIN.
- Stage 3: At the end of three days, the new files on the Master Server will become available to the member machines in R&D DOMAIN. Those

machines will, in turn, automatically update and run with the new software. The member machines will make the software available to the production machines after four more days pass.

- Stage 4: After a total of seven days, the files will be made available to our production machines, which will retrieve them and automatically update their software.

Stage 1 - Downloading the files

Our first step is to retrieve the latest InocuLAN virus signatures and software updates. The AutoDownload Manager program handles the acquisition of virus signatures and software updates from the Cheyenne site by using FTP or modem connections.

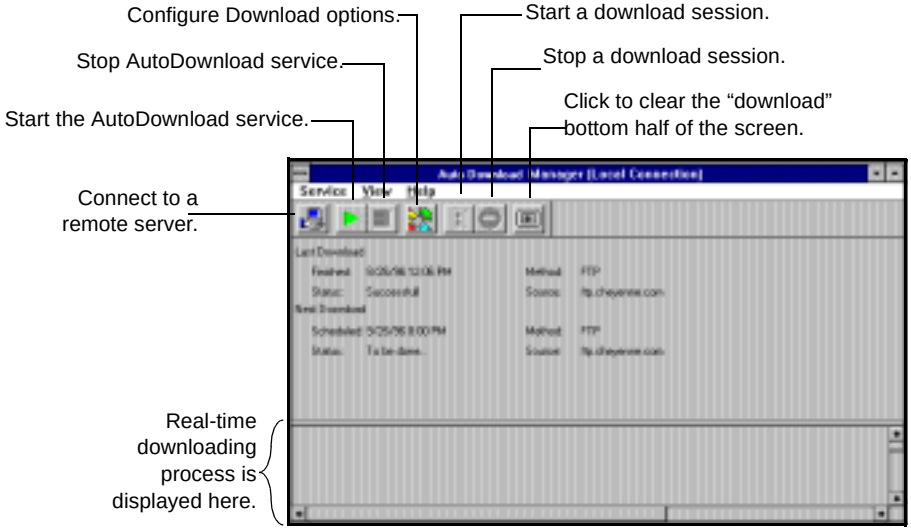
The AutoDownload Manager allows the user to change the default download date and time. InocuLAN is shipped with a monthly update setting.

NOTE: When first installing InocuLAN 4, it is recommended that you run a manual file download to ensure that the most current files are available. The AutoDownload service should be configured to start automatically on the machine you will be using for downloading. This can be done using the Control Panel.

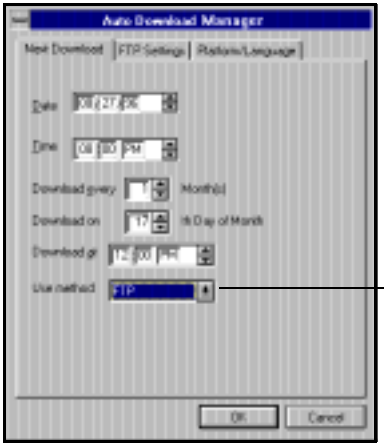
We begin by configuring the Master Server on R&D DOMAIN to download the new files:

1. **We start the AutoDownload Manager icon from the Program Manager in Windows NT 3.51 or from the Start menu under Programs, InocuLAN for Windows NT in Windows NT 4.0.**

The AutoDownload main screen will appear showing the last and next download to take place:



2. Next, we click on the Download option toolbar button.



Click on the combo-box and select either *Modem (BBS)* or FTP to connect to the Cheyenne site.

NOTE: The minimum scheduled download period is one month.

The *Next Download* tab allows us to schedule the time, date, and month of the download.

3. Two methods of downloading are available.

„ We can use FTP to connect to the Cheyenne site. The correct FTP site address is "ftp.cheyenne.com". We also enter our email address in the *Email Address* field.

„ We can also connect using a dialup asynchronous modem. If we highlight "Modem (BBS)" from the *Use method* sub-menu, the FTP Settings tab will change to *Modem Settings*.

Our modem information would be entered in the appropriate fields. The *First Name*, *Last Name*, and *Password* fields default to the correct information.

4. **Next we click on the *Platform/Language* tab.**

Because we have a large network that has multiple platforms and languages, we will select and download all the available files.

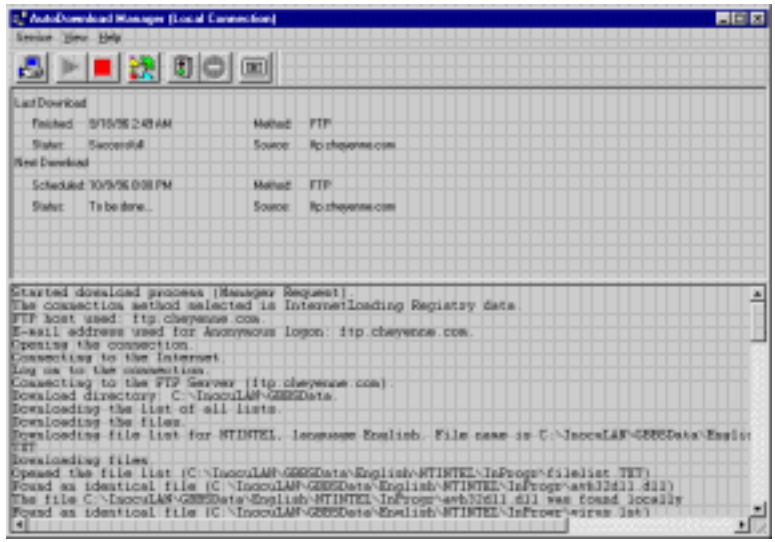
5. **Click OK when completed.**

6. **Before the download takes place, we must start the service by clicking the Start AutoDownload service toolbar button.**

When the service has been started, the "traffic light" toolbar button will become active. We click this button to run the download session immediately, rather than waiting for a scheduled time.

NOTE: The AutoDownload *Service* should not be mistaken for the AutoDownload download *session*. The service, like other Windows NT services, must be started before any actual client/server activity can occur.

When the downloading has completed, a screen similar to the one below is displayed:



The downloaded files are stored in the GBBSdata sub-directory. *Note that AutoDownload only retrieves the files from Cheyenne Software.* It does not distribute them. File distribution is a separate process (see next section for details).

7. The download session is complete, and we exit AutoDownload.

NOTE: The AutoDownload service is still running. Only the download "interface" or manager has been closed. You can always start up the AutoDownload manager to view the upcoming download schedule or configurations without having to restart the AutoDownload service.

It is recommended that the AutoDownload service be configured for automatic startup on all machines that will be used for downloads. This value is set through the Control Panel.

Summary of Stage 1:

As Stage 2 begins, we have completed AutoDownload and retrieved updates for all languages and platforms. These files are residing in the **GBBSdata** sub-directory of InocuLAN on the R&D DOMAIN master server. *At this time, the files have not yet entered the InocuLAN system*. The AutoDownload process only retrieves the files, it does not distribute them.

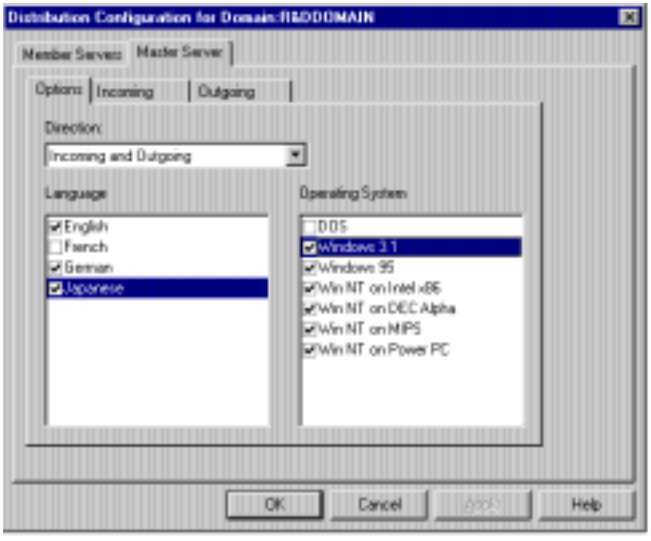
The next step will be to update the Master Server of R&D DOMAIN.

Stage 2 - Updating the Master Server

To begin the process:

1. **Start up the Service Manager from the Quick Start menu.**

2. **Click on the Configure Distribution Subsystem button. The options screen appears:**



3. **We are configuring the Master Server in R&D DOMAIN, so we select the Master Server tab.**

4. **Because we want to control both the incoming and outgoing settings, we select *Incoming and Outgoing* in the Direction field.**

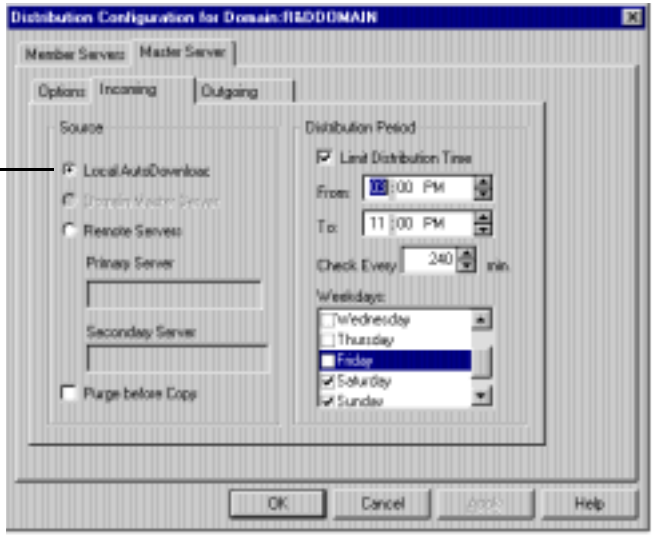
> ### Distribution Tips
>
> It is very important to understand the meaning of **Incoming** and **Outgoing** in the software distribution system.
>
> *Incoming* parameters determine from where to get files, when to get them, and how often to check for them. These files can be retrieved from the local AutoDownload directory (GBBSdata) or from another InocuLAN machine.
>
> *Outgoing* refers to the files that a given server makes available to other InocuLAN machines.

5. **While our enterprise uses all of the listed languages, the French network is currently undergoing repair. Therefore, we are temporarily not updating those machines, and we deselect *French* in the Languages field. (Note that we did download the French updates because we want to have them available. They will remain in the GBBSdata directory.)**

6. **Because no one in our enterprise is using DOS-based machines, we deselect *DOS* in the Operating Systems field.**

7. **The next step is to determine from where (the Source) and when (the Distribution Period) the files will enter the InocuLAN system. Click on the *Incoming* tab.**

This will retrieve files from the local GBBSdata directory.



8. **Since we downloaded the files to the InocuLAN Master Server and now want to bring those files into the InocuLAN system, we select *Local AutoDownload:* i.e., we will use the files on this machine's hard drive, stored in GBBSdata.**

9. **If we had used the Distribution function before, there might already be files that were moved into the InocuLAN system. We can eliminate those files by choosing the *Purge Before Copy* function. If we do not select this option, identically named files will be overwritten, and other files will remain.**

10. **Because we don't want the Master Server getting files during the week, we will restrict the distribution/ update to the weekend.**

    To do so, we select *Limit Distribution Time,* and under Weekdays choose *Saturday* and *Sunday.* However, our

full system backups take place early on Saturday morning. Therefore, we further limit the distribution time by choosing *From 3:00 PM to 11:00 PM*. This will leave ample time for our backups in the morning, and for file distribution in the afternoon.

Summary of Stage 2:

With these settings, the Master Server will retrieve the new software updates after 3:00 PM on Saturday from the local GBBSdata directory. (The GBBSdata directory is only accessed locally.) Upon retrieving the files, the Master Server will begin the update process. (*Only* the Master Server is updating at this time.) During the update, the InocuLAN service will be temporarily stopped to allow files to be copied. Upon completion, the service will restart automatically.

In the next step we will configure the outgoing parameters so that the Master Server runs with the new software for three days before other machines are given access.

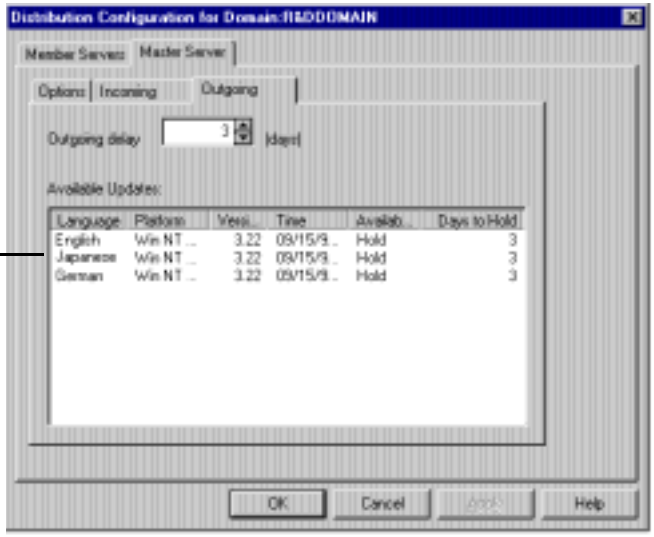
Stage 3 - Updating the R&D DOMAIN member machines

1. **Before other machines can retrieve files from the Master Server, the Outgoing parameters must be set. Click on the Master Server Outgoing tab:**

   Outgoing determines when other machines in our InocuLAN network can get new files from the machine we are configuring.

   To prevent the member machines (Member1, Member2 and Member3) from accessing the software too soon, we set *Outgoing delay* on the Master Server to three days. Doing so will hold the files on the Master Server for three days before they will be distributed to rest of R&D DOMAIN. Remember that the three day delay does not apply to the Master

Because we did not include French language files in the Incoming settings, they are not available for distribution.



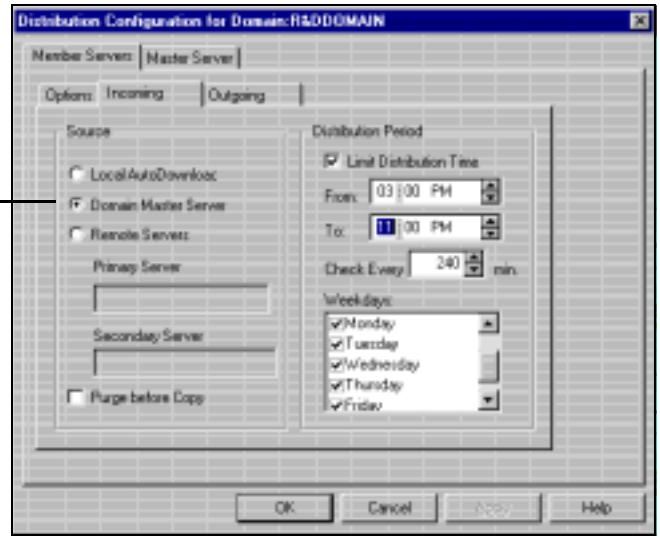
Server, which has already been updated with new software.

2. **Click on OK when completed.**

3. **The next step is to configure the member machines to retrieve software from the Master Server.**

4

Click on the *Member Servers* tab, and select *Incoming*.



Files will be retrieved from the Domain Master Server.

4. **Since the domain member machines will retrieve their update files from the domain Master Server, we click the *Domain Master Server* button as the Source.**

   As we recall, the Master Server received its files on Saturday and will hold them for three days: that is, they will be made available on Tuesday.

5. **Because we plan to update our production network four days from now using the files on the R&D DOMAIN member machines, we click the *Outgoing* tab for the *Member Servers* and set the *Outgoing Delay* to four days.**

Summary of Stage 3:

The member servers in R&D DOMAIN are now configured to take the new software from the Master Server. After the Master Server's three day Outgoing Delay passes, the member machines will access the software, copy it, and begin the updating process. The member machines, as the Master Server did, will shut down briefly while the updates take place, and automatically restart afterwards.

The member machines will run the new software for four days, at which time it will be made available to the production network.

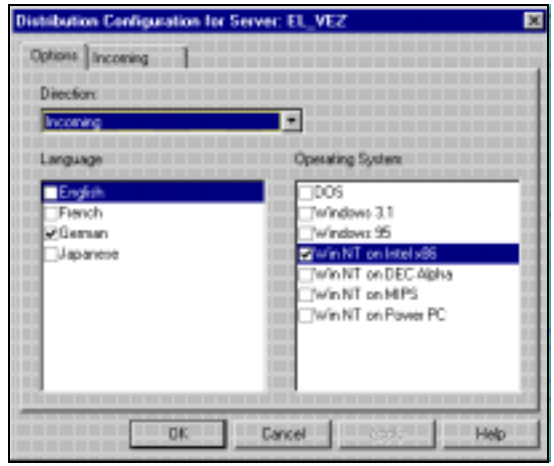
So far, Stage 2 and Stage 3 have allowed us seven days of running the software in our test environment. We have scheduled a seven-day cycle in order for the production machines to update on Saturday, one week after the process began, when they are not heavily used.

Stage 4 - Updating the Production network

The final stage is to move the new software into the production network.

All of our InocuLAN machines and InocuLAN domains will be configured to retrieve software from the R&D DOMAIN machines. A great deal of variation is possible at this point. The steps below will illustrate some of the possibilities.

1. **The first production machine configured is named El_Vez. Because El_Vez is a German language, Intel-based Windows NT machine, we need only retrieve that configuration. On the Options tab of El_Vez, we select *German* and *Win NT on Intel x86*.**



2. **We decide that El_Vez should retrieve its files from machine MEMBER1 of R&D DOMAIN. In the *Primary Server* field, we enter MEMBER1. As a precaution, we enter MEMBER2 in the *Secondary Server* field.**

3. **Because El_Vez is a production machine that should only update on weekends, we click *Limit Distribution Time* and the *Saturday* and *Sunday* buttons under Weekdays.**

   We have left the time at the default settings because we are not concerned about what time on the weekend the update will occur.

4. **Since no other machines will be retrieving files *from* El_Vez, we do not set any Outgoing parameters.**

   Click OK to set the parameters.

5. **We continue to similarly configure all the InocuLAN machines in our enterprise, each one set to retrieve precisely the version of the software that it requires.**

Summary of Stage 4:

When all our production machines are configured, the entire enterprise has been automated.

In sum, each month the following will occur:

- The R&D DOMAIN Master Server will automatically contact the Cheyenne Software FTP site and download the latest InocuLAN updates.
- The Master Server will update itself on the first Saturday following the download. It will run the software for three days.
- On the following Tuesday, the member machines in R&D DOMAIN will update with software retrieved from the Master Server. They will run an additional four days.
- One week after the process began, all machines in our InocuLAN production network will retrieve the correct software and update automatically.

Thus configured, the InocuLAN network requires no user intervention to always have the most current virus

signature files and software updates running on all machines.

Updating of Client Workstations

Windows 95, Windows 3.x and DOS clients are updated when they log in to a Windows NT domain set up to run the AVUPDATE program from a login script. (Please see the Release Notes for details about AVUPDATE.)

NOTE: For details on AVUPDATE Configuration settings for InocuLAN for NetWare, please refer to the “AVUPDATE User Guide” documentation.

ALERTING USERS WHEN A VIRUS IS DETECTED

In this chapter, you will learn:

Alert basics

What is Alert?

Alert is a notification system that sends messages from InocuLAN and other Cheyenne products to persons in your organization using different methods of communication. These messages (status, warning, and errors) can be sent to the system administrator, a hardware technician, or anyone else, in or out of the office. An individual or groups of persons in different segments of the network can also be notified.

How does Alert work with InocuLAN?

Alert does not generate its own messages. For example, InocuLAN generates warning messages whenever a virus is detected. These warning messages are passed to Alert, which sends the notification.

Alerts can be sent via:

- Broadcasts - Alert broadcasts can be sent to specific NT machines or NT domains.
- Pager - Numeric and alphanumeric.
- Electronic Mail - Microsoft Mail, Microsoft Exchange and Lotus Notes.
- Trouble Tickets - An alert can be printed through any print queue on your network.
- Simple Network Management Protocol (SNMP) managers - Such as NetWare Management System (NMS) and HP OpenView.
- Local and Remote NT Event Log Notification.
- CA-Unicenter TNG Option- Send a message to the TNG console and/or World View repository when an alert is generated.

In addition, Alert 4.0 features include:

- Remote Management and Configuration of Alert Service.
- Alerts from clients may now be sent using IP in addition to the standard IPX protocol.
- Messages containing full paths of the virus-ridden files.

NOTE: Alert 4.0 is compatible with other Cheyenne products. Any configurations previously set will not be overwritten. It is recommended that you run Alert and verify your settings before running InocuLAN.

What are the components of Alert?

Alert has two basic components:

- ALERT SERVICE - This is the Service that is responsible for the reception, processing, and distribution of alert messages.
- ALERT MANAGER - This is where you can configure how Alert broadcasts its messages.

Running the Alert Manager

To view and/or modify Alert settings:

1. **For Windows NT 3.51 users, double-click on the Alert Manager icon in the InocuLAN for Windows NT Group.**

   For Windows NT 4.0 users, click Start, then InocuLAN, then Alert.

   The Alert Manager screen appears:

Pressing the arrow button will start the Alert Service immediately. Once the service is running, the toolbar button is grayed out. The Alert Service must be started BEFORE items can be added or edited.

Stops the Alert Service.

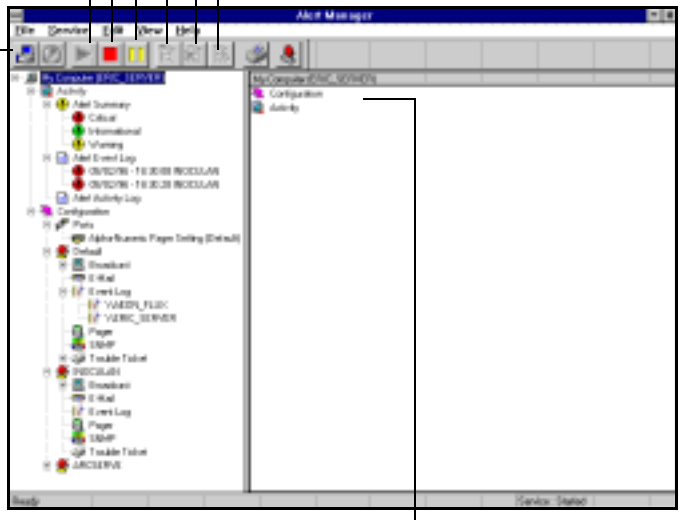
Pauses the Alert Service. You can still add/edit items.

Create a new item for the highlighted Alert mechanism.

Delete a highlighted item.

Edit a highlighted option.

Click to connect to a remote machine.



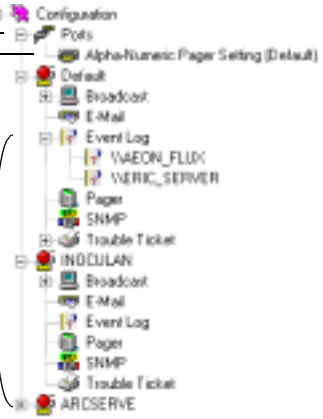
Information regarding the left-hand Function tree is displayed here.

A closer look at the Alert Parameter Tree.

Function Leaf Object

Option Leaf Object

Available Item(s) Object



Click on the [+] to expand the application specific recipient information. Click on [-] to collapse that part of the tree.

5

Configuring Alert

Alert allows for the configuration of the default settings. These settings are used by all the applications that use the Alert Service. You can also enter configuration information specifically for an individual application, which will override the default Alert configuration. Each application that uses Alert is displayed as a leaf on the left-hand function tree.

Starting the Alert Service

In order to display or configure Alert, it is necessary to start the Alert Service.

1. **Click on the Alert Service tool-bar button.**

   Plus signs will appear under the “My Computer” leaf object once the Alert Service has been started.

2. **Click on the plus signs to expand the function and options object leaves.**

Establishing a Service Account connection

The Alert Service must be able to communicate with the Windows NT server, otherwise Alerts will not be sent.

An account must be created by the Windows NT Administrator that has "Log on as a Service" user rights. The domain, user name, and password for that Windows NT account must be entered. If such a login does not exist when Alert is first started, the Service Login Settings dialog box will appear.

This will be grayed-out, unless you have installed the Microsoft Exchange client.

To login the Alert Service:

1. **Pull down the Service menu and select "Set Service Account".**

NOTE: The Alert Service must be started, as shown on page 5-7, before Set Service Account can be accessed.

The Service Logon Settings dialog box will be displayed.

2. **Enter the Domain, User name, and password you plan to use with the Alert service.**

3. **If you are running the Microsoft Exchange Client, the server name and mailbox must be specified.**

> **NOTE:** This mailbox must be associated with the specified account.

4. **Click on OK to save the information.**

Editing and creating Port configurations

The *Ports* object, located under the Configuration object, contains communication port profiles. Port configurations are used by the Pager and any function that utilizes serial port access.

When adding a new Port object:

1. **Select the "Ports" leaf object located under the "Configuration" leaf for the desired machine.**
2. **Right-click to display the pop-up menu and select "New Item."**

When editing a current Port configuration object:

1. **Expand the "Ports" leaf object. Select the configuration you wish to edit.**
2. **Right-click to display the pop-up menu and select "Edit Item."**
3. **Click OK when completed.**

The following fields are configured:

Port	Select the communications port being used.
Baud Rate	Select the baud rate.
Parity	Select the parity setting: NONE, ODD, or EVEN.
Data Bits	Select the number of data bits, 7 or 8.
Stop Bits	Enter the number of stop bits, 1 or 2.

NOTE: For numeric pagers, the recommended settings are: 8 data bits, NO parity, 1 stop bit. For alphanumeric pages, the recommended settings are: 7 data bits, EVEN parity, 1 stop bit. Consult the pager's user guide if you encounter any problems with the pager communication.

Using the Broadcast option

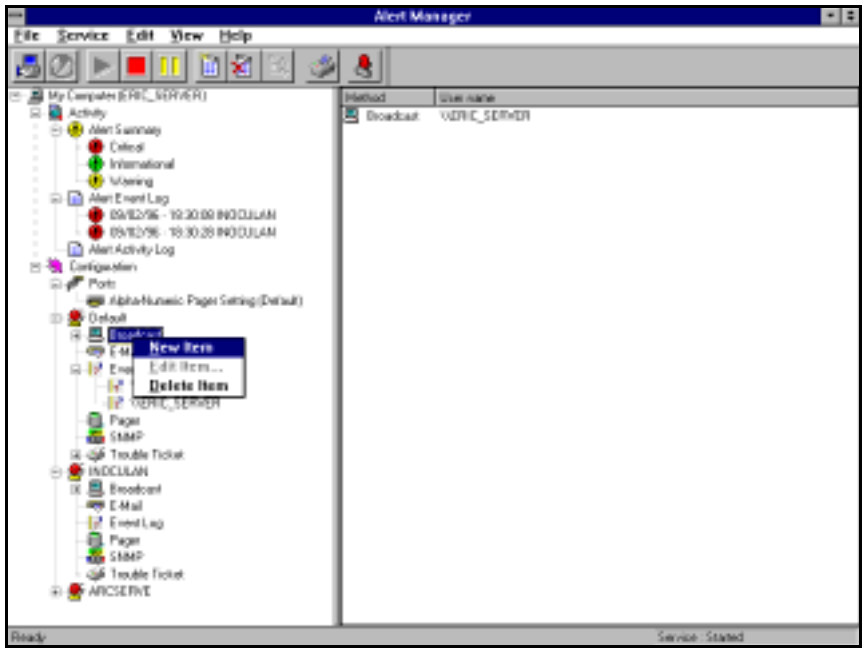
Alert broadcasts can be sent to specific network users or groups when InocuLAN detects a virus on your network.

Adding broadcast recipients

To add broadcast recipients:

1. **In the Alert Manager, click the Broadcast name on the left-hand side of the screen.**

2. **Right-click to display the context menu and select "New Item."**



The Broadcast Recipient box is displayed.

3. **You can select an entire Windows NT domain or expand a domain to reveal its servers.**

Select a domain or an individual server and click the Add button to add it to the recipient list.

4. Click the OK button when you have completed the broadcast recipient additions.

The Broadcast information is displayed on the right side of the Alert main screen.

Method	Recipient
Broadcast	\\NTBUILD
Broadcast	BUILD
Broadcast	\\NT-DAN
Broadcast	\\ERIC_SERVER
Broadcast	\\DELPHI

Using the Pager option

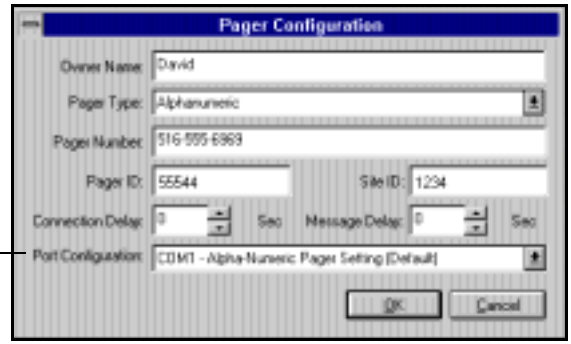
The pager option is used to a send a pager message when a virus is detected. Both numeric and alphanumeric pagers can be used at the same time.

Adding pager recipients

1. **Select the "Pager" leaf object located under the "Configuration" leaf for the desired machine.**

2. **Right-click to display the pop-up menu and select "New Item."**

   The Pager Configuration screen appears.



The Port Configuration is set through the Ports object.

Owner name

Enter the name of the Pager Recipient.

Pager Type

Indicate if you are using a numeric or alphanumeric pager.

Pager Number

Enter a maximum of 24 characters. If a digit, such as 9, is needed for a dial tone, it must be included in this field.

A comma can be entered to indicate a one second pause. If a longer pause is desired, a string of commas can be entered.

A dash (-) can be used to separate digits, but it has no function. (Since this can vary by modem, you should verify this with your modem manual.)

Pager ID

Enter up to eight digits to identify the pager that will receive the alerts.

Site ID

Enter up to four digits to identify where the alert occurred. This ID is included in the message to the pager. Therefore, if the number is less than four digits, you should use leading zeros.

Connection Delay

Enter the number of seconds you want to wait before a connection is made with the pager company. This will vary with your pager company, location, time of day, telephone equipment, and telephone traffic. If the connection is not established immediately, adding a delay can prevent the alert from being sent before the connection is established.

Message Delay

Enter the number of seconds to wait between the time the connection is made and the alert message is sent.

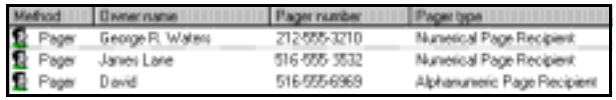
Port Configuration

Select the appropriate Port configuration from the drop down list. This configuration profile can be edited and additional pager profiles can be created. These pager configuration profiles are stored under the *Ports* leaf object.

NOTE: When sending an alphanumeric message, consult your paging service for proper modem settings. The Alert service requires the TAP protocol for alphanumeric pages.

3. Click OK to save your information.

The pager recipients are displayed on the right side on the Alert Manager screen.



Method	Owner name	Pager number	Pager type
Pager	George R. Waters	212-555-3210	Numerical Page Recipient
Pager	James Lane	516-555-3532	Numerical Page Recipient
Pager	David	516-555-6969	Alphanumeric Page Recipient

4. **Double-clicking on each recipient's name under the *Pager* object displays all the pager information for the selected item.**

Interpreting the numeric pager message

When a numeric pager is sent because of a virus alert, the coded message will appear as: **Message = DDSSSSCC**

DD is the virus detection code number. It tells you which component of InocuLAN has detected a virus.

You must check InocuLAN's scanning records to determine which machine is infected and which files or directories contain the virus.

Virus Detection Code	Description
01	WIMMUNE detected viral activity on a local machine. Viral activity includes: Unauthorized reformatting of the hard disk, a change in the boot sector, or a change in the partition table.
02	WIMMUNE detected a virus in a local file.
03	A boot virus or a change to the Critical Disk Area was detected on a local machine.
04	The InocuLAN Manager detected a virus at a local machine.
05	The InocuLAN Server detected a virus on a machine.
07	WIMMUNE detected a virus in memory.
08	WIMMUNE detected a boot virus.

SSSS is the user defined site number from the Pager Configuration screen. The site number represents the machine that detected the virus.

CC is the user defined custom code from the Pager Configuration screen. The custom code represents the machine that sent the message.

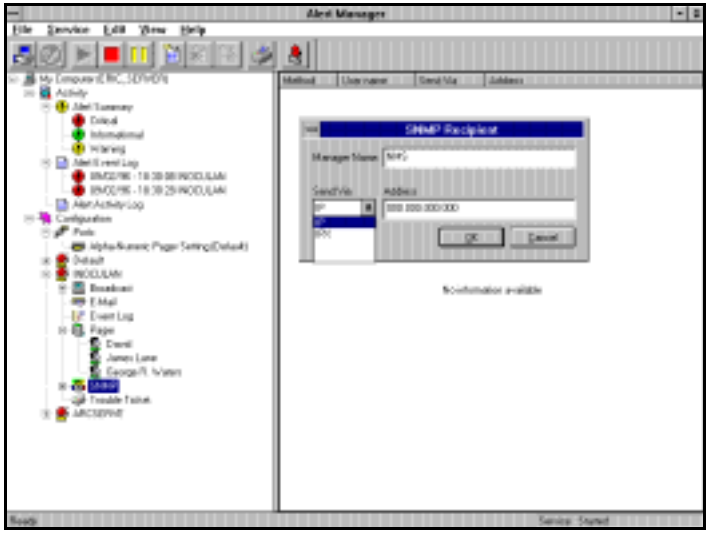
Using the SNMP option

The SNMP option is used to send an SNMP 'trap' (message) to an SNMP manager when an alert is generated. Examples of SNMP managers include NetWare Management System (NMS) and HP OpenView.

1. **Highlight the SNMP leaf object to display the current SNMP settings on the right-hand side.**

Label	Data
User name	NMS
Send Via	IP
Method	SNMP
Address	...

2. **Click on the *Edit Item* or *New Item* toolbar button (or use the right click menu) to edit/configure the SNMP recipient.**



3. Enter information on the SNMP Configuration screen.

Manager Name — Enter the name of the SNMP Manager.

Via IPX — Select IPX and enter the 8 byte network address of the machine where the SNMP manager is located. Next, enter the 12 byte node address of the machine where the SNMP manager is located. Use this field for Novell networks.

Via IP — Select IP and enter the IP address of the machine where the SNMP manager is located. Use this field if you are running the TCP/IP stack.

3. Click OK to save your information.

NOTE: The Management Station must be configured to receive the alert. Please consult the Release Notes for information about several SNMP managers.

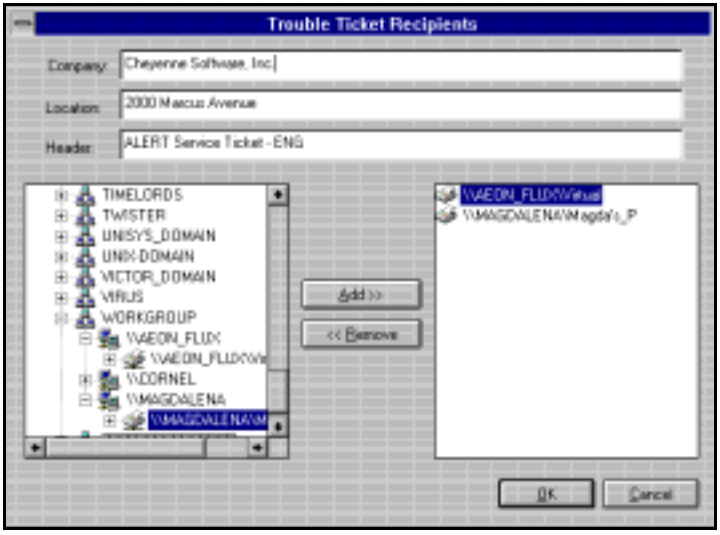
Using the Trouble Ticket option

Trouble tickets are used to alert users through a printed document.

To create a Trouble Ticket:

1. **Highlight the *Trouble Ticket* leaf object.**

2. **Click on the Edit Item or New Item toolbar button (or use the right-click menu).**



Recipient Browser.

Type in the following information into the above fields.

Company/Location — Enter the name of your company and its location.

Header — Enter the information that should appear at the top of each Trouble Ticket.

Recipient

3. **Use the browser to select the printer recipient.**

   Highlight the chosen printer.

4. **Click Add to move that printer on to recipient list.**

   You will be prompted to provide the username and password to connect to the printer device.

5. **To add additional recipients, repeat steps 3 and 4.**

   Click OK to save the information.

   The information is displayed.

Method	Server name	Print queue	Connect As
Trouble Ticket	\\MAGDALENA	Magda's_P	guest
Trouble Ticket	\\AEON_FLUX	Virtual	guest

Using the E-mail option

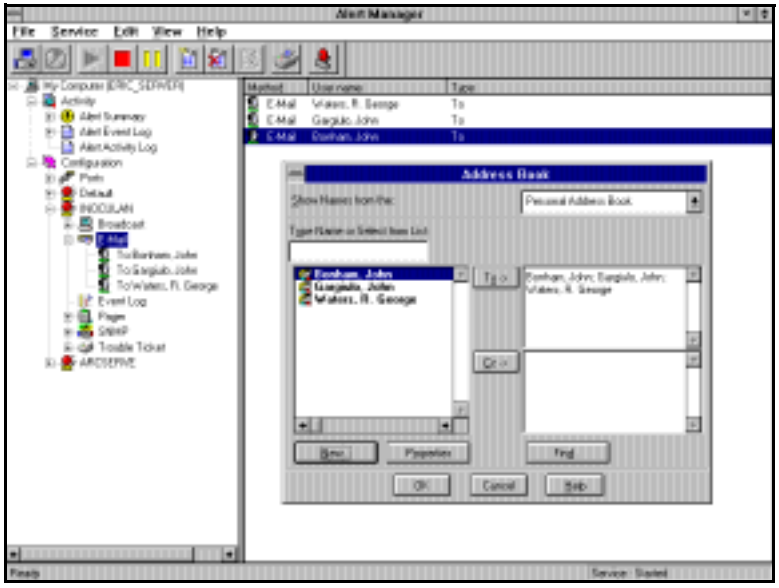
The E-mail option is used to send E-mail messages to specific users when a virus is detected. If the Microsoft Exchange Client is installed, Alert will support only the Microsoft Exchange Server.

To setup the E-mail recipients:

1. **Highlight the *E-Mail* leaf under the *INOCULAN* object.**

2. **Click on the *New Item* toolbar button**

   The mail login dialog box will appear:



3. **Select the E-mail recipients using the dialog provided by the mail system.**

4. **Click OK to save the information.**

Assigning Attachments to E-mail Messages

File attachments can be added to the E-mail messages that are sent to the selected recipients. This can be used to inform the users of what steps to take in a viruses was found.

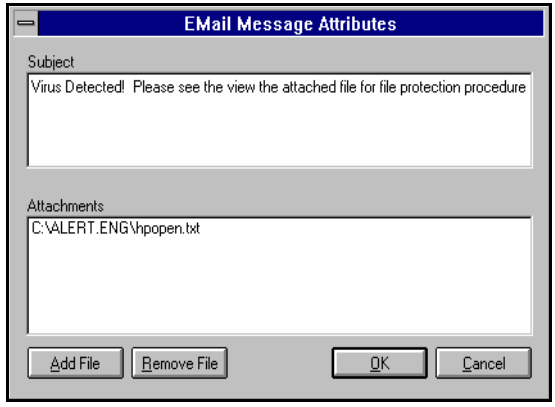
To assign attachments to the message and define a subject heading:

1. **Select the E-mail leaf object.**

2. **Right click to display the pop-up menu.**

3. **Select *Message Attributes*.**

   The message attributes box will appear:



4. **Enter a short subject heading.**

5. **Click on *Add File*.**

   Select the file(s) you wish to attachments and click OK.

6. **Click OK to save the attachments.**

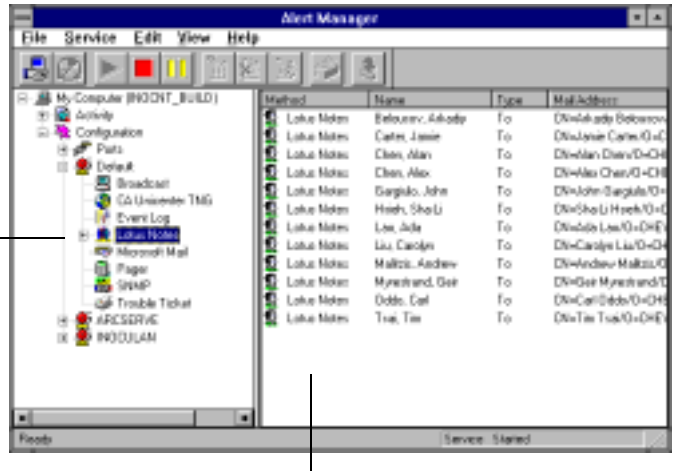
NOTE: Click on the E-mail leaf object and select Message Attributes to review or add any additional attachments.

Using the Lotus Notes Option

The Lotus Notes Option makes it possible to send a message to a Lotus Notes user when an alert is generated.

To send an Alert message to a Lotus Notes user:

1. **Highlight the Lotus Notes leaf object to display the current Lotus Notes settings on the right-hand side.**



Lotus Notes Settings

To set the configuration settings for the Alert service:

2. **Right click the Lotus Notes leaf object to bring up the context menu and select the Lotus Notes settings.**

   The following screen appears:.

3. **Enter the path where Lotus Notes is installed.**

4. **Enter the password.**

   If you want the service to switch to another User Id, check Specific account and supply the next three fields:

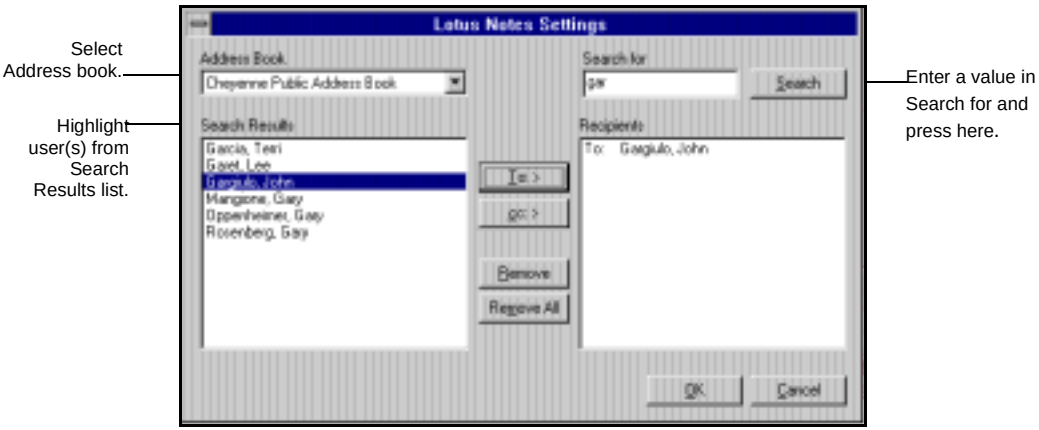
   - Id file
   - Mail Server
   - Mail File

Click OK upon completion of these steps.

Lotus Notes Recipients

From the Alert Manager screen, click on the *Edit Item* or *New Item* toolbar button (or use the right click menu) to edit/configure the Lotus Notes recipient.

The following screen appears:



5. **Select an Address Book from the pulldown list of the Lotus Notes Settings dialog.**

6. **Enter a value to Search for, and then press the Search button or Enter key.**

   The Search is performed on the Fullname Field of the Address book.

7. **Select your prospective Lotus Notes Alert recipient from the Search Results list.**

8. **Select To:> or cc:> to add a user to the recipient list.**

   Select Remove to remove a user.

9. **Select Remove All to delete all recipients.**

   Click OK upon completion of the above steps.

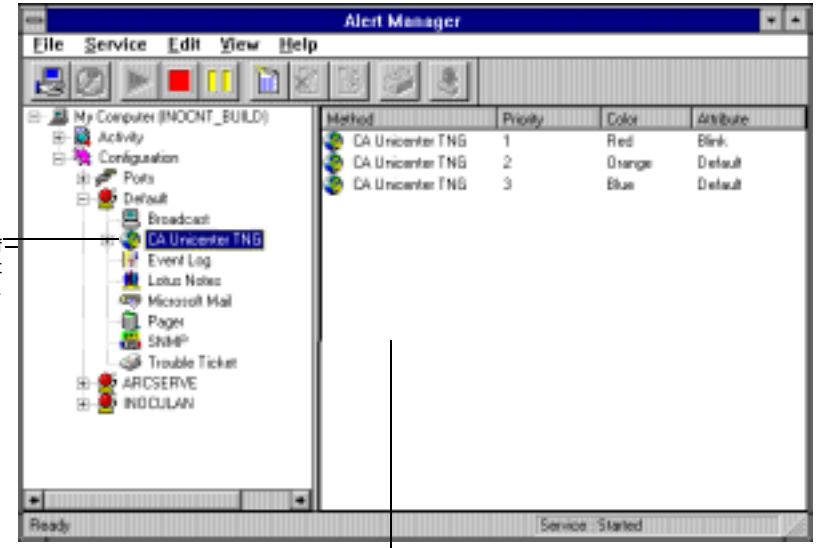
Using the CA-Unicenter TNG Option

The CA-Unicenter TNG (The Next Generation) Option makes it possible to send a message to the CA-Unicenter TNG console and/or World View repository when an alert is generated.

To send a message to the CA-Unicenter TNG Console and/or the World View repository:

1. **Highlight the CA-Unicenter TNG leaf object to display the current CA-Unicenter TNG Settings on the right-hand side.**

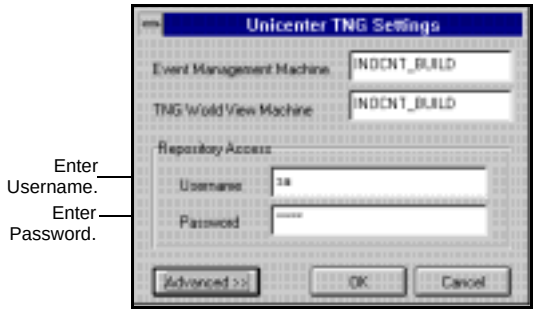
   The following screen appears:



TNG Settings

2. **Right click the CA-Unicenter TNG leaf object to bring up the context menu and select CA-Unicenter TNG Settings.**

The following screen appears:



3. Enter the Event Management Machine and CA-Unicenter TNG World View Machine names.

The Event Management machine identifies the computer running the Unicenter Event Management console. The TNG World View machine identifies the computer containing the World View repository.

If the World View machine is the same as the computer that you are running Alert on, enter the username and password for access to the CA-Unicenter TNG repository.

Click on OK.

NOTE: The Alert application must be running on both the Event Management machine as well as the World View machine if specified in the Unicenter TNG settings dialog.

---

4. If you click on the Advanced button, the dialog will expand to show the following screen:

By selecting Advanced, the user can thereby define the class name for the application.

Mappings can be created, edited or deleted.

5. Configure Advanced Application/Class Map settings at this point.

Application refers to the application (in this case InocuLAN) sending the alert.Class refers to the type of object (in this case InocuLAN) in CA-Unicenter TNG and is case-sensitive.

This Advanced information is useful for those administrators familiar with the TNG repository and the definition of class types.

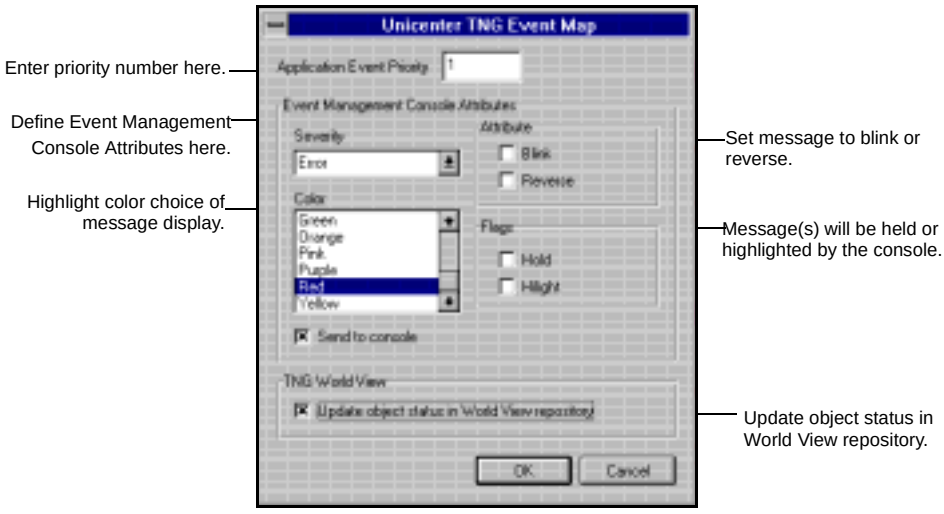
You can now create a New mapping, Edit an existing mapping, or Delete a mapping.

Click OK to set these changes.

TNG Recipients

6. From the Alert Manager screen, click on the *Edit Item* or *New Item* toolbar button (or use the right click menu) to edit/configure the CA-Unicenter TNG recipient.

The following screen appears:



7. Enter the Application Event Priority.

Currently, all applications calling Alert specify an Event Priority from the following table:

ALERT SPECIFICATIONS

Events Priority	Description
1	ERROR
2	WARNING
3	INFORMATION

8. Define the settings using the Event Management Console Attributes section of the dialog.

Within TNG you can define the attributes for the console messages received from your machine.

Select the attributes, colors, etc., you want and check Send to console.

9. **To tell Alert to search for the Application object in the TNG repository, check the Update object status box in World View repository.**

   Click OK to complete these steps.

Sample TNG Alert Scenarios

If you want to send informational alerts to the CA-Unicenter TNG Console using blue text, for example, configure a recipient as follows:

Event Priority	Description
3	Application Event Priority
Blue	Color
☑	Send to Console

If you want to send error alerts to the CA-Unicenter TNG Console using red text, and have the object status in the World View repository updated, configure another recipient as follows:

Event Priority	Description
1	Application Event Priority
Red	Color
☑	Send to Console
☑	Send to World View

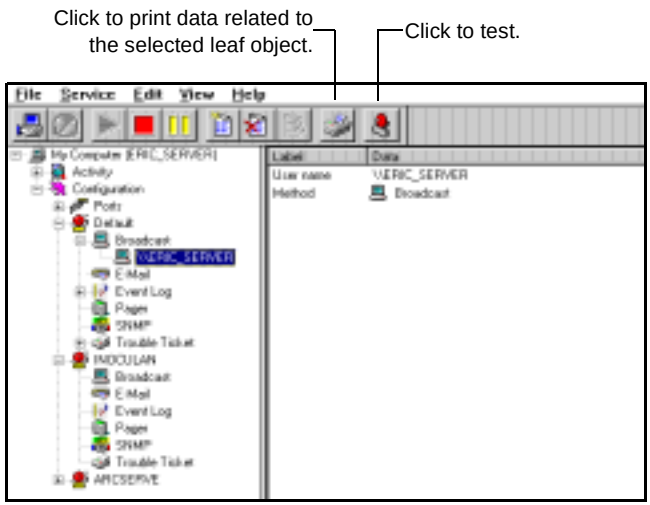
Testing the Recipients

The Test toolbar button lets you test any of the Alert messaging functions without there actually being an “alarm” condition.

You should test any features after the configuration has been completed.

To avoid unnecessary alarm, inform any Alert recipients that a test is taking place.

1. **Highlight the Alert recipients.**



2. **Click on the test button.**

The test Alert will be sent to selected recipients.

Alert's Activity Log

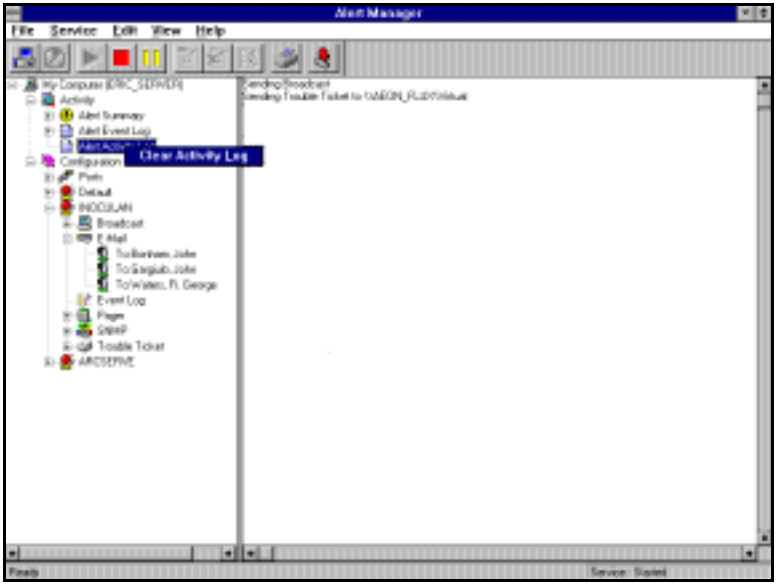
A historical listing is stored in the Activity Log. You can view, print, or clear this log.

Displaying the Activity Log

To display the Activity Log:

1. **Highlight the Activity Log object from the Alert manager tree.**

   The contents of the activity log are displayed in the right pane:



2. **Right-click and select Clear Activity Log to delete the contents of the activity log. You might want to do this if Alert has been running for a long time and the log has grown too large.**

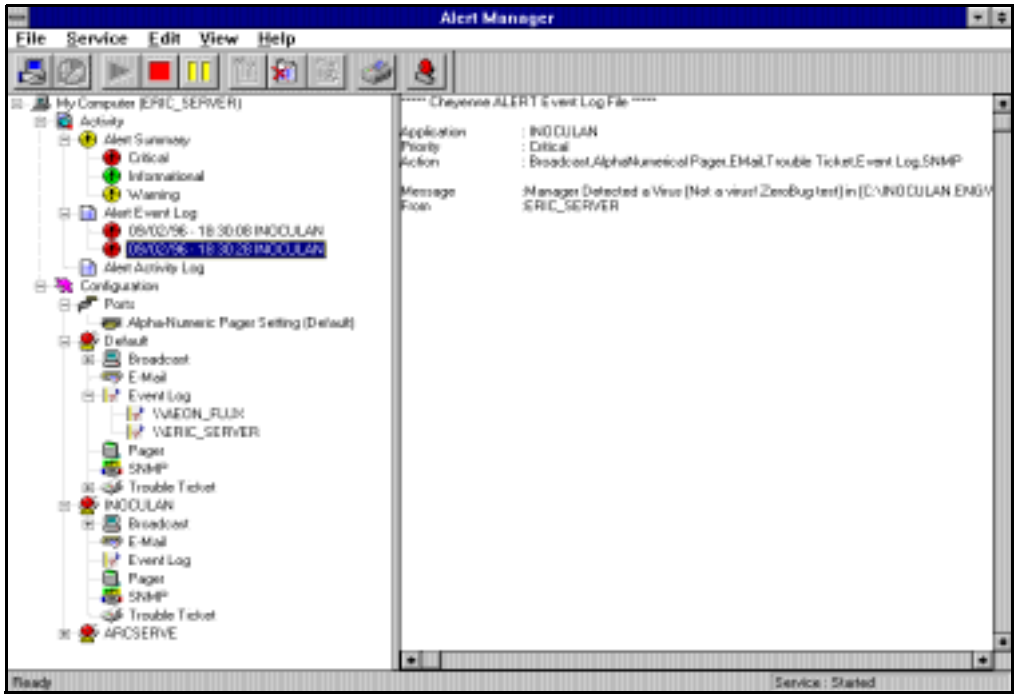
Alert's Event Log

Every message that Alert sends on behalf of all applications is stored in the Event Log. You can view, print, or clear this log.

Displaying the Event Log

To display the Event Log:

1. **Highlight the Alert Event Log object. The information will appear on the right side of the screen.**

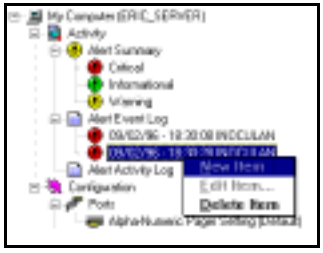


Clearing the Messages Report Log

You can delete the Event Log. You might want to do this if Alert has been running for a long time and the log has grown too large.

To clear the log:

1. **Highlight the Event object and right-click.**



2. **Select Delete Item to remove the Event Log.**

Fields on the Event Log screen

Date\Time — Displays the date and time the event occurred.

Description — The description is determined by the applications that set the alert.

Application — Tells you the application that generated the event.

Printing selected objects

Any selected leaf object's data can be printed by selecting the *Print* command from the **File** menu or print button on the toolbar.

K

L

M

N

O

P

R

S

T

V

W

Z